

05. 3. 2004

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 3 年 4 月 3 日

出 願 番 号  
Application Number: 特 願 2 0 0 3 - 1 0 0 8 6 6  
[ST. 10/C]: [ J P 2 0 0 3 - 1 0 0 8 6 6 ]

出 願 人  
Applicant(s): 松下電器産業株式会社

REC'D 22 APR 2004

WIPO

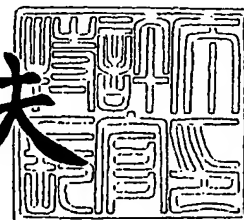
PCT

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2 0 0 4 年 4 月 9 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



【書類名】 特許願  
【整理番号】 2054051008  
【あて先】 特許庁長官殿  
【国際特許分類】 H04L 9/032  
G07C

## 【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社  
社内

【氏名】 ▲浜▼井 信二

## 【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

## 【代理人】

【識別番号】 100109210

## 【弁理士】

【氏名又は名称】 新居 広守

【電話番号】 06-4806-7530

## 【手数料の表示】

【予納台帳番号】 049515

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0213583

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信装置、証明書発行装置及び通信システム

【特許請求の範囲】

【請求項 1】 サーバ装置の正当性を示すサーバ証明書に基づいて前記サーバ装置と通信する通信装置であって、

前記サーバ証明書の有効性を判断する基準となる情報である失効番号を保持するリポジトリ装置から、前記失効番号を取得する失効番号取得手段と、

取得された失効番号を記憶する失効番号記憶手段と、

前記サーバ証明書を識別する識別番号を前記サーバ証明書から読み出す識別番号読み出し手段と、

読み出された識別番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記サーバ証明書の有効性を判断する証明書判断手段と、

前記サーバ証明書が有効であると判断された場合に、前記サーバ装置との通信を確立し、前記サーバ証明書が有効でないと判断された場合に、前記サーバ装置との通信を確立しない通信制御手段と

を備えることを特徴とする通信装置。

【請求項 2】 前記有効性判断手段は、前記識別番号が前記失効番号と同じか大きい場合に、前記サーバ証明書が有効であると判断する

ことを特徴とする請求項 1 記載の通信装置。

【請求項 3】 前記通信装置は、さらに、前記失効番号の有効性を判断する失効番号判断手段を備え、

前記証明書判断手段は、前記失効番号判断手段によって前記失効番号が有効であると判断された場合に、前記失効番号を用いて、前記サーバ証明書の有効性を判断する

ことを特徴とする請求項 1 記載の通信装置。

【請求項 4】 前記失効番号判断手段は、前記リポジトリ装置の正当性を示すリポジトリ証明書の識別番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記失効番号の有効性を判断する

ことを特徴とする請求項 3 記載の通信装置。

【請求項 5】 前記失効番号判断手段は、前記識別番号が前記失効番号と同じか大きい場合に、前記リポジトリ装置が有効であると判断することを特徴とする請求項 4 記載の通信装置。

【請求項 6】 前記失効番号判断手段は、前記失効番号取得手段によって取得された失効番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記失効番号取得手段によって取得された失効番号の有効性を判断する

ことを特徴とする請求項 3 記載の通信装置。

【請求項 7】 前記失効番号判断手段は、前記失効番号取得手段によって取得された失効番号が前記失効番号記憶手段に記憶されている失効番号と同じか大きい場合に、前記失効番号が有効であると判断する

ことを特徴とする請求項 6 記載の通信装置。

【請求項 8】 サーバ装置の正当性を示すサーバ証明書を発行する証明書発行装置であって、

サーバ証明書の有効性を判断する基準となる情報である失効番号を記憶する失効番号記憶手段と、

新たなサーバ証明書を発行する発行手段とを備え、

前記発行手段は、前記失効番号記憶手段に記憶されている失効番号と同じか大きい値を示す識別番号を含ませて、前記サーバ証明書を発行する

ことを特徴とする証明書発行装置。

【請求項 9】 前記証明書発行装置は、さらに、失効させるサーバ証明書の識別番号の通知を取得すると、前記失効番号記憶手段に記憶されている失効番号を前記識別番号よりも大きい番号に更新する失効番号更新手段を備える

ことを特徴とする請求項 8 記載の証明書発行装置。

【請求項 10】 前記証明書発行装置は、さらに、サーバ証明書の有効期限が近づいたサーバ証明書の識別番号を特定し、前記失効番号記憶手段に記憶されている失効番号を前記識別番号よりも大きい番号に更新する失効番号更新手段を備える

ことを特徴とする請求項 8 記載の証明書発行装置。

【請求項 11】 前記発行手段は、前記失効番号更新手段によって失効番号が更新された場合に、更新後の失効番号よりも小さな値の識別番号をもつサーバ証明書に対応するサーバ装置に対して、新たなサーバ証明書を発行する

ことを特徴とする請求項 9 又は 10 記載の証明書発行装置。

【請求項 12】 サーバ装置と、サーバ装置の正当性を示すサーバ証明書を発行する証明書発行装置と、前記サーバ証明書に基づいて前記サーバ装置と通信する通信装置とから構成される通信システムであって、

前記証明書発行装置は、

サーバ証明書の有効性を判断する基準となる情報である失効番号を記憶する失効番号記憶手段と、

新たなサーバ証明書を発行する発行手段とを備え、

前記発行手段は、前記失効番号記憶手段に記憶されている失効番号と同じか大きい値を示す識別番号を含ませて、前記サーバ証明書を発行し、

前記通信装置は、

前記サーバ証明書の有効性を判断する基準となる情報である失効番号を保持するリポジトリ装置から、前記失効番号を取得する失効番号取得手段と、

取得された失効番号を記憶する失効番号記憶手段と、

前記サーバ証明書を識別する識別番号を前記サーバ証明書から読み出す識別番号読み出し手段と、

読み出された識別番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記サーバ証明書の有効性を判断する証明書判断手段と、

前記サーバ証明書が有効であると判断された場合に、前記サーバ装置との通信を確立し、前記サーバ証明書が有効でないと判断された場合に、前記サーバ装置との通信を確立しない通信制御手段と備える

ことを特徴とする通信システム。

【請求項 13】 サーバ装置の正当性を示すサーバ証明書に基づいて前記サーバ装置と通信する通信方法であって、

前記サーバ証明書の有効性を判断する基準となる情報である失効番号を保持するリポジトリ装置から、前記失効番号を取得する失効番号取得ステップと、

取得された失効番号を記憶手段に格納する失効番号格納ステップと、  
前記サーバ証明書を識別する識別番号を前記サーバ証明書から読み出す識別番号読み出しステップと、  
読み出された識別番号と前記記憶手段に記憶されている失効番号とを比較することによって前記サーバ証明書の有効性を判断する証明書判断ステップと、  
前記サーバ証明書が有効であると判断された場合に、前記サーバ装置との通信を確立し、前記サーバ証明書が有効でないと判断された場合に、前記サーバ装置との通信を確立しない通信制御ステップと  
を含むことを特徴とする通信方法。

【請求項 14】 サーバ装置の正当性を示すサーバ証明書を発行する証明書発行方法であって、

サーバ証明書の有効性を判断する基準となる情報である失効番号を記憶手段に格納する失効番号記憶ステップと、

新たなサーバ証明書を発行する発行ステップとを含み、

前記発行ステップでは、前記記憶手段に記憶されている失効番号と同じか大きい値を示す識別番号を含ませて、前記サーバ証明書を発行する

ことを特徴とする証明書発行方法。

【請求項 15】 サーバ装置の正当性を示すサーバ証明書に基づいて前記サーバ装置と通信する通信装置のためのプログラムであって、

前記サーバ証明書の有効性を判断する基準となる情報である失効番号を保持するリポジトリ装置から、前記失効番号を取得する失効番号取得ステップと、

取得された失効番号を記憶手段に格納する失効番号格納ステップと、

前記サーバ証明書を識別する識別番号を前記サーバ証明書から読み出す識別番号読み出しステップと、

読み出された識別番号と前記記憶手段に記憶されている失効番号とを比較することによって前記サーバ証明書の有効性を判断する証明書判断ステップと、

前記サーバ証明書が有効であると判断された場合に、前記サーバ装置との通信を確立し、前記サーバ証明書が有効でないと判断された場合に、前記サーバ装置との通信を確立しない通信制御ステップと

をコンピュータに実行させることを特徴とするプログラム。

【請求項 16】 サーバ装置の正当性を示すサーバ証明書を発行する証明書発行装置のためのプログラムであって、

サーバ証明書の有効性を判断する基準となる情報である失効番号を記憶手段に格納する失効番号記憶ステップと、

新たなサーバ証明書を発行する発行ステップとをコンピュータに実行させ、

前記発行ステップでは、前記記憶手段に記憶されている失効番号と同じか大きい値を示す識別番号を含ませて、前記サーバ証明書を発行する

ことを特徴とするプログラム。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、通信装置、証明書発行装置及び通信システム等に関し、通信時においてサーバ証明書を用いてサーバ認証を行う通信装置、証明書発行装置及び通信システム等に関する。

##### 【0002】

##### 【従来の技術】

インターネットにおけるサーバ・クライアント間の通信時における盗聴、サーバなりすましに対抗する技術としてSSL (Secure Socket Layer) が特許文献1に、SSLを改良したTLS (Transport Layer Security) が特許文献2に記載されている（以下総称してSSLと呼ぶ）。

##### 【0003】

図15は、SSL通信時における通信システムのシステム構成を示すブロック図である。

##### 【0004】

通信システムは、認証局 (CA) が運営するサーバ証明書作成装置1000及びリポジトリ2000と、アプリケーション提供者が使用する複数のアプリケーションサーバ3000a～3000kと、ユーザが使用する複数の端末4000

a～4000nとから構成される。リポジトリ2000、各アプリケーションサーバ3000a～3000k及び各端末4000a～4000nは、インターネット5000に接続されている。

#### 【0005】

サーバ証明書作成装置1000は、各端末4000a～4000nに対してCA証明書6000を発行したり、アプリケーションサーバ3000a～3000kに対してサーバ証明書7000を発行したり、リポジトリ2000に対してサーバ証明書無効化リスト（以下、「CRL」とも記す。）8000を配信したりするコンピュータ装置である。

#### 【0006】

リポジトリ2000は、配信を要求した端末4000a～4000nに対してCRL8000を配信するコンピュータ装置であり、サーバ証明書作成装置1000から配信されてきたCRL8000を蓄積するCRL蓄積部2100と、各端末4000a～4000nからの配信要求を受け付けて、CRL蓄積部2100に蓄積されているCRL8000を配信を要求した端末4000a～4000nに対して送信する通信部2200とを備える。

#### 【0007】

各アプリケーションサーバ3000a～3000kは、SSL通信時に通信を要求した端末4000a～4000nに対してサーバ証明書7000を配信するコンピュータ装置であり、サーバ部3100と、サーバ証明書蓄積部3200と、通信部3300とを備える。

#### 【0008】

各端末4000a～4000nは、クライアント部4100と、CA証明書蓄積部4210及びCRL蓄積部4220を有するサーバ証明書検証部4200と、時計4300と、通信部4400とを備える。

#### 【0009】

端末4000a～4000nがアプリケーションサーバ3000a～3000kと通信を行うまえにあらかじめ認証局はサーバ証明書作成装置1000でサーバ証明書を発行し、各アプリケーションサーバ3000a～3000kにサーバ



証明書 7000 を配布する。アプリケーションサーバ 3000a～3000k は配布されたサーバ証明書 7000 をサーバ証明書蓄積部 3200 に蓄積する。

#### 【0010】

また、サーバ証明書 7000 を署名する CA の秘密鍵のペアとなる CA の公開鍵を含む CA 証明書 6000 を端末 4000a～4000n に配布し、端末 4000a～4000n は CA 証明書 6000 を CA 証明書蓄積部 4210 に蓄積する。

#### 【0011】

一方、認証局は、サーバ証明書 7000 の無効を調査し、無効と判断すればサーバ証明書作成装置 1000 でそのサーバ証明書 7000 のシリアルをリストに加えた新たな CRL 8000 を作成し、リポジトリ 2000 に配布する。

#### 【0012】

リポジトリ 2000 は、CRL 蓄積部 2100 に CRL 8000 を蓄積する。端末 4000a～4000n は、定期的にリポジトリ 2000 の通信部 2200 に CRL 8000 の配信を要求する。

#### 【0013】

端末 4000a～4000n からの要求に応じて CRL 8000 を端末 4000a～4000n に配布する。リポジトリ 2000 は CRL 蓄積部 2100 から CRL 8000 を取り出し、CRL 8000 を通信部 2200 から端末 4000a～4000n の通信部 4400 に送信する。端末 4000a～4000n は受信した CRL 8000 を CA 証明書蓄積部 4210 に保管する。

#### 【0014】

図 16 は、図 15 に示されるサーバ証明書 7000 の最小限の構成例を示す図である。なお、SSL ではサーバ証明書として x509 形式が使用される。

#### 【0015】

サーバ証明書 7000 は、バージョン 7001 と、シリアル 7002 と、署名アルゴリズム 7003 と、発行者 7004 と、有効期間 7005 と、名前 7006 と、公開鍵 7007 と、署名 7008 とから構成される。

#### 【0016】

バージョン 7001 は、x509 のバージョンを示す。シリアル 7002 は、発行者によってサーバ証明書に付与されるユニークな番号である。署名アルゴリズム 7003 は、発行者が署名する際のアルゴリズムを示す。発行者 7004 は、このサーバ証明書を発行した認証局の名前である。有効期間 7005 は、サーバ証明書が有効な期間を示す。名前 7006 は、サーバ証明書の発行先の名前である。公開鍵 7007 は、サーバの公開鍵である。署名 7008 は、このサーバ証明書の署名を除く部分に対して認証局が認証局の CA 秘密鍵を用いて署名した署名である。

#### 【0017】

図 17 は、図 15 に示される CRL 8000 の最小限の構成を示す図である。

CRL 8000 は、バージョン 8001 と、署名アルゴリズム 8002 と、発行者 8003 と、更新時間 8004 と、次回更新時間 8005 と、失効証明書 8006 と、署名アルゴリズム 8007 と、署名 8008 とから構成される。

#### 【0018】

バージョン 8001 は、失効証明書リストのバージョンである。署名アルゴリズム 8002 は、発行者が署名した際のアルゴリズムを示す。発行者 8003 は、CRL 8000 の発行者である認証局の名前である。更新時間 8004 は、この失効証明書リストの発行された時間であり、次回更新時間 8005 は、次に更新する予定時間である。失効証明書 8006 は、失効したサーバ証明書のシリアル 8006a とその失効時間 8006b のリストである。認証局が発行者の名前で発行したサーバ証明書のうち、認証局が失効したと判断したサーバ証明書のシリアルがシリアル 8006a にその失効した時間 8006b とともに記載される。署名アルゴリズム 8007 は、発行者が署名した際のアルゴリズムを示す。署名 8008 は、CRL 8000 の署名を除く部分に対して認証局が CA 秘密鍵を用いて署名した署名である。

#### 【0019】

次いで、端末 4000a ~ 4000n 及びアプリケーションサーバ 3000a ~ 3000k 間で暗号化せずに通信を行う場合について説明する。

#### 【0020】

図18は、暗号化せずに通信を行う場合のシーケンス図である。なおここでは、端末4000aとアプリケーションサーバ3000aとの間で行われた場合をその代表例として説明する。

【0021】

端末4000aのクライアント部4100は、アプリケーションサーバ3000aに対してリクエスト1を送るように通信部4400に指示をする(S801)。通信部4400は、アプリケーションサーバ3000aの通信部3300に対してリクエスト1を送信する(S802)。

【0022】

アプリケーションサーバ3000aの通信部3300は、受信したリクエスト1をサーバ部3100に出力する(S803)。サーバ部3100はリクエスト1を処理してレスポンス1を生成し、端末4000aに送るよう通信部3300に指示する(S804)。通信部3300は、端末4000aの通信部4400にレスポンス1を送信する(S805)。

【0023】

端末4000aの通信部4400は、レスポンス1をクライアント部4100に出力する(S806)。

【0024】

このようなシーケンスでリクエスト1、レスポンス1が暗号化されずに通信が行われる。

【0025】

次に端末4000a～4000n及びアプリケーションサーバ3000a～3000k間で暗号化して通信を行う場合について説明する。

【0026】

図19は、暗号化して通信を行う場合のシーケンス図である。なおここでは、端末4000aとアプリケーションサーバ3000aとの間で行われた場合をその代表例として説明する。

【0027】

端末4000aのクライアント部4100は、リクエスト2を暗号化してアプ

リケーションサーバ3000aに送るよう通信部4400に指示を行う(S900)。通信部4400は、共有鍵の種のひとつとなるクライアント乱数と通信部4400が処理できる暗号の種類を含んだClientHelloパケットをアプリケーションサーバ3000aの通信部3300に送信し、SSLのハンドシェークを開始する(S901)。

#### 【0028】

アプリケーションサーバ3000aの通信部3300は、ClientHelloパケットから暗号の種類を決定し、共有鍵の種の一つとなるサーバ乱数とこの通信を一意に特定するセッションIDを生成し、決定した暗号の種類とサーバ乱数とセッションIDをServerHelloパケットで送り(S902)、サーバ証明書蓄積部3200からサーバ証明書を取り出し(S903)、サーバ証明書7000をCertificateパケットとして端末4000aの通信部4400に送信し(S904)、さらにServerHelloDoneパケットを通信部4400に送る(S907)。

#### 【0029】

端末4000aの通信部4400は、Certificateパケットからサーバ証明書7000を取り出し、サーバ証明書検証部4200に送る(S905)。サーバ証明書検証部4200は、サーバ証明書が不正でないか検証し、検証結果を通信部4400に通知する(S906)。サーバ証明書が不正であれば、通信部4400は、アラートパケットをアプリケーションサーバ3000aの通信部3300に送信して通信を切断し、クライアント部4100にエラーを返す。これに対して、サーバ証明書が不正でない場合には、通信部4400は、暗号化の共有鍵を計算するためのプリマスターシークレットを作成して、サーバ証明書7000に含まれるサーバ公開鍵で暗号化し、ServerHelloDoneパケットの到着後に暗号化されたプリマスターシークレットを含むClientKeyExchangeパケットをアプリケーションサーバ3000aの通信部3300に送信し(S908)、さらにChangeCipherSpecパケットを通信部3300に送信する(S909)。ChangeCipherSpecパケットは、暗号化の開始を示すパケットである。通信部4400は、ク

クライアント乱数とサーバ乱数とプリマスターシークレットから暗号化に使用する共通鍵Cを作成し、ハンドシェークの終了を示すF i n i s h e dパケットを作成した共通鍵Cで暗号化してアプリケーションサーバ3000aの通信部3300に送信する(S910)。

#### 【0030】

アプリケーションサーバ3000aの通信部3300は、C l i e n t K e y E x c h a n g eから暗号化されたプリマスターシークレットを取り出し、サーバ秘密鍵を用いてプリマスターシークレットに復号し、サーバ乱数、クライアント乱数とともに暗号化に使用する共通鍵Dを作成する。SSLのハンドシェークが正常に行われた場合、通信部3300の持つ共通鍵Cと通信部4400の持つ共通鍵Dは同一となる。通信部3300は、受信したF i n i s h e dパケットを共通鍵Dで復号し、正常に復号できればF i n i s hパケットを暗号化して端末4000aの通信部4400に送信する(S911)。このF i n i s h e d以降の通信は、すべて暗号化して行われる。

#### 【0031】

端末4000aの通信部4400は、受信したF i n i s h e dパケットを復号し、正常に復号できれば、リクエスト2を暗号化してアプリケーションサーバ3000aの通信部3300に送付する(S912)。

#### 【0032】

アプリケーションサーバ3000aの通信部3300は、リクエスト2を復号し、サーバ部3100に送る(S913)。サーバ部3100は、リクエスト2を処理してレスポンス2を生成し、端末4000a~4000naに送るよう通信部3300に指示する(S914)。通信部3300は、端末4000aの通信部4400にレスポンス2を暗号化して送信する(S915)。

#### 【0033】

端末4000aの通信部4400は、レスポンス2を復号してクライアント部4100に出力する(S916)。

以上のように暗号化を行い通信する。

#### 【0034】

次いで、サーバ証明書検証部 4200 が行う検証について説明する。

図 20 は、サーバ証明書検証部 4200 が行うサーバ証明書 7000 の検証動作を示すフローチャートである。

#### 【0035】

サーバ証明書検証部 4200 は、受信したサーバ証明書 7000 から有効期間 7005 を取り出し、また時計 4300 から現在時刻を取得する（S9051）。次いでサーバ証明書検証部 4200 は、有効期間 7005 の始期及び終期と現在時間をそれぞれ比較し、現在時間がサーバ証明書の有効期間 7005 でなければ期限外のエラーコードを通信部 4400 に通知して検証を終了する（S9057）。

#### 【0036】

これに対して現在時間がサーバ証明書の有効期間 7005 内であれば、サーバ証明書 7000 の発行者 7004 を取り出し、さらに保管している CA 証明書蓄積部 4210 から、発行者 7004 の CA 証明書 6000 を検索する。発行者の CA 証明書 6000 があればその CA 証明書 6000 から CA の公開鍵を取り出し、CA の公開鍵を用いてサーバ証明書 7000 の署名 7008 のチェックを行う。署名 7008 が不正であれば、署名の検証エラーのエラーコードを通信部 4400 に通知して検証を終了する（S9057）。

#### 【0037】

署名（1208）が正しければ、サーバ証明書検証部 4200 は、サーバ証明書 7000 からシリアル 7002 を取り出す。そして CRL 蓄積部 4220 から CRL 8000 を取り出し、取り出したシリアルが CRL 8000 に含まれているかどうかをチェックする。もし含まれていればそのサーバ証明書は失効していると判断し、失効のエラーコードを通信部 4400 に通知して検証を終了する（S9057）。もし含まれていないならばそのサーバ証明書は正しいと判断して通信部 4400 に正常終了を通知する。

#### 【0038】

以上のように端末 4000a～4000n はアプリケーションサーバ 3000 と通信する際に SSL を用いた暗号化通信を行い、盗聴とサーバのなりすましを

防止する。

【0039】

【特許文献1】

U. S. P a t e n t    5 6 5 7 3 9 0

【0040】

【特許文献2】

R F C 2 2 4 6 ( I E T F )

【0041】

【発明が解決しようとする課題】

しかしながら、従来の方法では次の点に課題がある。

【0042】

まず、従来の通信システムではCRLの大きさが固定でなく、サーバ証明書の失効が増えるとともにCRLのサイズが非常に大きくなる（数十～数百kバイト）。このことから端末においてCRLを蓄積する容量として大きなものを用意しなければならないという課題がある。また、CRLが大きくなった場合、サーバ証明書の検証時にサーバ証明書のシリアルがCRLのリストに含まれているかどうか検索する時間が大きくなるという課題がある。また、CRLが大きくなった場合、端末がリポジトリからCRLを取得する際の通信路の容量及びリポジトリの処理能力に大きなものが必要となるという課題がある。

【0043】

さらにサーバ証明書の有効期間検証の際に現在時間と比較するために正確な時計が必要であるという課題がある。

【0044】

すなわち、サーバ装置の正当性を示すサーバ証明書に基づいて当該サーバ装置と通信するため、従来のシステムでは端末（通信装置）などに容量の大きなメモリや、精度の高い時計、通信インターフェースなど十分なリソースが必要であった。

【0045】

本発明は、上述の技術的課題を解決し、簡単なリソースでサーバ装置の正当性

を示すサーバ証明書に基づいて当該サーバ装置と通信することができる通信装置、証明書発行装置及び通信システム等を提供することを目的とする。

#### 【0046】

##### 【課題を解決するための手段】

上記目的を達成するために、本発明に係る通信装置は、サーバ装置の正当性を示すサーバ証明書に基づいて前記サーバ装置と通信する通信装置であって、前記サーバ証明書の有効性を判断する基準となる情報である失効番号を保持するリポジトリ装置から、前記失効番号を取得する失効番号取得手段と、取得された失効番号を記憶する失効番号記憶手段と、前記サーバ証明書を識別する識別番号を前記サーバ証明書から読み出す識別番号読み出し手段と、読み出された識別番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記サーバ証明書の有効性を判断する証明書判断手段と、前記サーバ証明書が有効であると判断された場合に、前記サーバ装置との通信を確立し、前記サーバ証明書が有効でないと判断された場合に、前記サーバ装置との通信を確立しない通信制御手段とを備えることを特徴とする。

#### 【0047】

具体的には、前記有効性判断手段は、前記識別番号が前記失効番号と同じか大きい場合に、前記サーバ証明書が有効であると判断することを特徴としてもよい。

#### 【0048】

これにより、従来のようにサーバ証明書の有効期限が過ぎたか否かを時計を用いて判断したり、従来のようにリポジトリからサイズの大きなCRLを取得して、たくさんのリストを記憶し、このたくさんのリストの中にサーバ証明書の識別番号が載っているか否か検索したりする必要性がなくなり、通信装置は、リポジトリから失効番号を1つだけ取得し、これを記憶している1つの失効番号で、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。したがって、通信装置及びリポジトリのメモリ容量などのリソースが簡単で済み、簡単なリソースでサーバ装置の正当性を示すサーバ証明書に基づいて当該サーバ装置と通信することができる。



## 【0049】

また、前記通信装置は、さらに、前記失効番号の有効性を判断する失効番号判断手段を備え、前記証明書判断手段は、前記失効番号判断手段によって前記失効番号が有効であると判断された場合に、前記失効番号を用いて、前記サーバ証明書の有効性を判断することを特徴としてもよい。具体的には、前記失効番号判断手段は、前記リポジトリ装置の正当性を示すリポジトリ証明書の識別番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記失効番号の有効性を判断することを特徴とすることができ、また、前記失効番号判断手段は、前記識別番号が前記失効番号と同じか大きい場合に、前記リポジトリ装置が有効であると判断することを特徴とすることができる。

## 【0050】

これにより、通信装置は、サーバ装置との通信と同じ手順でリポジトリ証明書を取得し、リポジトリ証明書を用いてリポジトリを認証したり、リポジトリが正当である場合に失効番号を暗号通信で取得したり、正常な失効番号だけを取得して、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。

## 【0051】

また、前記失効番号判断手段は、前記失効番号取得手段によって取得された失効番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記失効番号取得手段によって取得された失効番号の有効性を判断することを特徴とすることができ、具体的には、前記失効番号判断手段は、前記失効番号取得手段によって取得された失効番号が前記失効番号記憶手段に記憶されている失効番号と同じか大きい場合に、前記失効番号が有効であると判断することを特徴とする。

## 【0052】

これにより、通信装置は、リポジトリが正当である場合に失効番号を暗号なしの通信で取得したり、正常な失効番号だけを取得して、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。

## 【0053】

また、サーバ装置の正当性を示すサーバ証明書を発行する証明書発行装置であって、サーバ証明書の有効性を判断する基準となる情報である失効番号を記憶する失効番号記憶手段と、新たなサーバ証明書を発行する発行手段とを備え、前記発行手段は、前記失効番号記憶手段に記憶されている失効番号と同じか大きい値を示す識別番号を含ませて、前記サーバ証明書を発行することを特徴とする。

#### 【0054】

具体的には、前記証明書発行装置は、さらに、失効させるサーバ証明書の識別番号の通知を取得すると、前記失効番号記憶手段に記憶されている失効番号を前記識別番号よりも大きい番号に更新する失効番号更新手段を備えることを特徴とすることができる。

#### 【0055】

これにより、従来のようにサーバ証明書の有効期限が過ぎたか否かを時計を用いて判断させたり、従来のようにリポジトリからサイズの大きなCRLを取得させたりして、たくさんのリストを記憶させたりし、このたくさんのリストの中にサーバ証明書の識別番号が載っているか否か検索させたりする必要がなくなり、通信装置は、リポジトリから失効番号を1つだけ取得し、これを記憶している1つの失効番号で、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。したがって、通信装置及びリポジトリのメモリ容量などのリソースが簡単で済み、簡単なリソースでサーバ装置の正当性を示すサーバ証明書に基づいて当該サーバ装置と通信することができる。

#### 【0056】

また、前記証明書発行装置は、さらに、サーバ証明書の有効期限が近づいたサーバ証明書の識別番号を特定し、前記失効番号記憶手段に記憶されている失効番号を前記識別番号よりも大きい番号に更新する失効番号更新手段を備えることを特徴とする。

#### 【0057】

これにより、有効期間が近づいたサーバ証明書を失効させることができる。

#### 【0058】

また、前記発行手段は、前記失効番号更新手段によって失効番号が更新された

場合に、更新後の失効番号よりも小さな値の識別番号をもつサーバ証明書に対応するサーバ装置に対して、新たなサーバ証明書を発行することを特徴とする。

#### 【0059】

これによりサーバ装置は、新たなサーバ証明書を用いて認証を受けることができる。

#### 【0060】

なお、本発明は、このような通信装置、証明書発行装置として実現することができるだけでなく、このサーバ装置と、サーバ装置の正当性を示すサーバ証明書を発行する証明書発行装置と、前記サーバ証明書に基づいて前記サーバ装置と通信する通信装置とから構成される通信システムとして実現したり、このような通信装置、証明書発行装置が備える特徴的な手段をステップとする通信方法、証明書発行方法として実現したり、それらのステップをコンピュータに実行させるプログラムとして実現したりすることもできる。そして、そのようなプログラムは、CD-ROM等の記録媒体やインターネット等の伝送媒体を介して配信することができるのは言うまでもない。

#### 【0061】

##### 【発明の実施の形態】

##### （実施の形態1）

以下、本発明の実施の形態1に係る通信システムについて説明する。

#### 【0062】

図1は、本発明の実施の形態1に係る通信システム1の全体構成を示すブロック図である。

#### 【0063】

この通信システム1は、公開鍵暗号方式を使って安全な通信を行うためのインフラPKI（Public Key Infrastructure）を提供するために、CA証明書60、サーバ証明書75及び失効情報90を基本のツールとして、アプリケーションサーバを認証するシステムであり、認証局（以下、「CA」とも記す。）が使用するサーバ証明書作成装置10及びリポジトリ20と、映像コンテンツなどのアプリケーション提供者が使用する複数のアプリケーションサーバ30a～30k

と、ユーザが使用する複数の端末 40a～40n と、リポジトリ 20、アプリケーションサーバ 30a～30k 及び端末 40a～40n を接続するインターネット 50 とから構成される。なお、各アプリケーションサーバ 30a～30k が同じ構成であるので同図においてはアプリケーションサーバ 30a の詳細構成だけが図示されており、また端末 40a～40n が同じ構成であるので同図においてはアプリケーションサーバ 30a の詳細構成だけが図示されている。

#### 【0064】

サーバ証明書作成装置 10 は、ワークステーション等のコンピュータ装置であり、通信システム 1 における基本のツールを提供する基本的なサーバとして機能する。具体的には、サーバ証明書作成装置 10 は、端末 40a～40n に対して CA 証明書 60 を予め発行したり、アプリケーションサーバ 30a～30k からの証明書要求 (Certificate Signing Request、以下、「CSR」とも記す。) 70 に応じて、「0」から「1」ずつ単調に増加され、かつこのシステムにおいてユニークなシリアルを含み、かつ各アプリケーションサーバ 30a～30k に専用のサーバ証明書 75 を発行したり、サーバ証明書 75 の有効期限が近づいたような場合においてサーバ証明書 75 を失効させるとき、該当するアプリケーションサーバに対して証明書失効 (証明書更新要求) を予め通知したり、「0」から必要数単調に増加され、サーバ証明書 75 が失効しているか否かを判断するためのシリアル (以下、「失効シリアル」あるいは「失効番号」とも記す。) を含む失効情報 90 をリポジトリ 20 に送信したりする。

#### 【0065】

なお、CA 証明書 60 は、例えばこの証明書の発行者と、署名アルゴリズムと、この証明書の有効期間 (例えば、10 年) と、CA の公開鍵 (CA 公開鍵) と、この CA 公開鍵とペアの CA の秘密鍵 (CA 秘密鍵) による署名とが含まれて構成されている。また、CSR 70 は、CSR を発したサーバの名前と、そのサーバの公開鍵 (サーバ公開鍵) とが含まれて構成されている。

#### 【0066】

リポジトリ 20 は、ワークステーション等のコンピュータ装置であり、サーバ証明書作成装置 10 から通知された最新の失効情報 90 を蓄積し、インターネッ

ト 50 を介して端末 40 a ~ 40 n から失効情報 90 の要求 (リクエスト) があると、要求した端末 40 a ~ 40 n に失効情報 90 をレスポンスとして暗号なしの通信で配信する。

#### 【0067】

アプリケーションサーバ 30 a ~ 30 k は、ワークステーション等のコンピュータ装置であり、サーバ証明書作成装置 10 から証明書失効通知があった場合など、必要に応じてサーバの名前及びそのサーバの公開鍵を含む CSR 70 をサーバ証明書作成装置 10 に対して行い、サーバ証明書作成装置 10 が発行した自己専用のサーバ証明書 75 を保持する。そして、アプリケーションサーバ 30 a ~ 30 k は、端末 40 a ~ 40 n からアプリケーションのダウンロードなどの要求 (リクエスト) があった際に SSL の通信プロトコルに従ってサーバ証明書 75 を送信し、認証を受けた後セッション鍵 (共有鍵) を用いて暗号通信で要求されたアプリケーションをレスポンスとして配信する。なお、暗号化せずに通信を行う場合は、従来と同様の手順が用いられる。

#### 【0068】

端末 40 a ~ 40 n は、ネット家電 (例えば、ビデオレコーダ) などのコンピュータ装置であり、サーバ証明書作成装置 10 が発行した CA 証明書 60 を予め取得し、これを保持する。また、各端末 40 a ~ 40 n は、リポジトリ 20 に対して定期的 (例えば 1 月に 1 回) の通信部 202 に失効情報 90 の配信を要求し、配信されてきた失効情報 90 に含まれる最新の失効番号を保持する。そして、端末 40 a ~ 40 n は、アプリケーションをダウンロードする際に SSL の通信プロトコルに従ってアプリケーションサーバ 30 a ~ 30 k から送信されてきたサーバ証明書 75 と、予め保持する CA 証明書 60 と、失効情報 90 の失効番号とに基づいてサーバを認証し、サーバ認証後セッション鍵を用いてリクエスト及びレスポンスを暗号通信する。

#### 【0069】

これによって、リクエスト及びレスポンスの盗聴とを防止する。

#### 【0070】

図 2 は、図 1 に示されるサーバ証明書 75 の構成例を示す図である。なお、こ

のサーバ証明書 75 においても、従来と同様、サーバ証明書として x509 形式が使用される。

#### 【0071】

このサーバ証明書 75 は、バージョン 751 と、シリアル 752 と、署名アルゴリズム 753 と、発行者 754 と、有効期間 755 と、サーバの名前 756 と、サーバ公開鍵 757 と、署名 758 との各フィールドから構成される。

#### 【0072】

バージョン 751 は、x509 のバージョンを示し、例えば「2」が格納される。シリアル 752 は、発行者によってサーバ証明書に付与されるユニークな番号であり、例えば「0x0011」（図示例では 2 バイト）が格納される。署名アルゴリズム 753 は、発行者が署名する際のアルゴリズムを示す。発行者 754 は、このサーバ証明書を発行した認証局の名前であり、例えば「Panasi gn」が格納される。有効期間 755 は、サーバ証明書が有効な期間を示し、例えばこのサーバ証明書 75 が発行された時刻（有効期間の始期、2003 年、4 月 1 日…）と、13 月後の時刻（有効期間の終期、2004 年、5 月 1 日…）とが格納される。名前 756 は、サーバ証明書の発行先の名前であり、例えば「針ウド映画」が格納される。サーバ公開鍵 757 は、サーバの公開鍵であり、例えば針ウド映画の公開鍵、Pubk\_\_11 が格納される。署名 758 は、このサーバ証明書の署名を除く部分の特徴、いわゆる指紋に対する署名であり、例えばサーバの名前針ウド映画とサーバ公開鍵 Pubk\_\_11 との連結を認証局の CA 秘密鍵で暗号化した値が格納される。

#### 【0073】

このように構成されたサーバ証明書 75 をアプリケーションサーバ 30a～30k からもらった端末 40a～40n は、署名 758 を認証局の CA 公開鍵で復号化することによって、サーバ証明書 75 が認証局によって正規に発行されたものかを検証したりすることが可能となる。

#### 【0074】

図 3 は、図 1 に示される失効情報 90 の構成例を示す図である。

#### 【0075】

図3に示されるように失効情報90は、発行者91と、失効番号92と、署名93の各フィールドから構成される。

#### 【0076】

発行者91は、失効情報90の発行者である認証局CAの名称であって、失効情報90が対象とするサーバ証明書75の発行者754と同一であり、P a n a s i g nが格納される。失効番号92は、発行者が発行しているサーバ証明書75の内、その時点で有効な最小のシリアルであり、例えば、0 x 0 0 1 1（図示例では2バイト）だけが格納される。署名93は、このサーバ証明書の署名を除く部分の特徴、発行者91及び失効番号92に対する署名であり、例えば発行者91と失効番号92との連結をCA秘密鍵で暗号化した値が格納される。

#### 【0077】

このように構成された失効情報90をリポジトリ20からもらった端末40a～40nは、署名93を認証局のCA公開鍵で復号化することによって、失効情報90が認証局によって正規に発行されたものかを検証したり、アプリケーションサーバ30a～30kからもらったサーバ証明書75のシリアルと失効番号92との大小関係とからそのサーバ証明書75が失効しているか否かを判断したりすることが可能となる。

#### 【0078】

次いで、サーバ証明書作成装置10、リポジトリ20、アプリケーションサーバ30a～30k及び端末40a～40nの各構成を順次さらに詳細に説明する。

#### 【0079】

図1に示されるようにサーバ証明書作成装置10は、鍵ペア作成部101と、CA証明書作成部102と、CA秘密鍵蓄積部103と、時計104と、シリアル蓄積部105と、CSR受信部106と、サーバ証明書組立部107と、署名部108と、サーバ証明書送信部109と、サーバ証明書履歴蓄積部110と、サーバ証明書期限検索部111と、サーバ証明書失効通知部112と、失効証明書検索部113と、証明書失効通知部114と、失効番号蓄積部115と、失効情報署名部116と、失効情報通知部117等とを備える。

**【0080】**

鍵ペア作成部101は、サーバ証明書75の署名を行うためのCA秘密鍵と、署名の検証を行うためのCA公開鍵とを作成する。そして鍵ペア作成部101は、作成したCA公開鍵及びCA秘密鍵をCA証明書作成部102に出力し、CA秘密鍵をCA秘密鍵蓄積部103に出力する。

**【0081】**

CA証明書作成部102は、鍵ペア作成部101で作成されたCA公開鍵などと、鍵ペア作成部101で作成されたCA秘密鍵で署名とでCA証明書60を作成し、端末40a～40nに送る。

**【0082】**

CA秘密鍵蓄積部103は、鍵ペア作成部101で作成されたCA秘密鍵を蓄積する。

時計104は、現在時刻を正確に計時する。

**【0083】**

シリアル蓄積部105は、次に発行するサーバ証明書75に付与されるべきシリアルを蓄積する。具体的には、サーバ証明書作成装置10でシリアル「4」のサーバ証明書75まで既に発行している場合には、シリアル蓄積部105は、シリアル「5」を蓄積する。なお、シリアル蓄積部105が蓄積するシリアルの初期値は「0」である。

**【0084】**

CSR受信部106は、各アプリケーションサーバ30a～30kからCSR70を受信すると、受信したCSR70をサーバ証明書組立部107に出力する。なお、CSR70は、サーバの名前及びサーバ公開鍵を含めて構成される。

**【0085】**

サーバ証明書組立部107は、サーバ証明書75に必要な情報を組み立てる。具体的には、サーバ証明書組立部107は、シリアル蓄積部105から読み出したシリアルをシリアル752に設定し、また時計104から取得した現在時刻を有効期間755の始期に設定し、現在時刻から13ヶ月後の時刻を有効期間755の終期、すなわち有効期限に設定する。そして、サーバ証明書組立部107は



、CSR70に含まれる名前及びサーバ公開鍵を名前756及びサーバ公開鍵757にそれぞれ設定し、予め定められたバージョン、発行者、署名アルゴリズムをバージョン751、発行者754、署名アルゴリズム753にそれぞれ設定し、サーバ証明書75に必要な情報を署名部108に出力する。

#### 【0086】

そして、サーバ証明書75に必要な情報を組み立てが終わると、サーバ証明書組立部107は、サーバ証明書75に必要な情報の内、名前756、シリアル752、有効期間755の終期（有効期限）を出力し、サーバ証明書履歴蓄積部110のサーバ証明書履歴テーブル110aに蓄積させる。さらに、サーバ証明書組立部107は、発行するサーバ証明書75のシリアルに1加えたもの（例えば、新規発行されるサーバ証明書75のシリアルが「0x0010」であれば「0x0011」）を次に付与すべきシリアルとしてシリアル蓄積部105に蓄積させる。

#### 【0087】

署名部108は、CA秘密鍵蓄積部103からCA秘密鍵を取り出し、サーバ証明書組立部107から出力されたバージョン751、シリアル752、署名アルゴリズム753、発行者754、有効期間755、名前756、サーバ公開鍵757に対して取り出したCA秘密鍵を関与させること署名758を作成し、サーバ証明書75を完成させた後、このサーバ証明書75をサーバ証明書送信部109に出力する。

#### 【0088】

サーバ証明書送信部109は、署名部108から出力されたサーバ証明書75をCSR70を発したアプリケーションサーバ30a～30kに送信する。この際、サーバ証明書送信部109は、新たなサーバ証明書75の送信を失効証明書検索部113に通知する。

#### 【0089】

サーバ証明書履歴蓄積部110は、サーバ証明書組立部107がサーバ証明書75を組み立てるごとに、そのサーバの名前、サーバ証明書のシリアル、有効期限をサーバ証明書履歴テーブル110aに順次蓄積する。

**【0090】**

図4は、サーバ証明書履歴蓄積部110が蓄積するサーバ証明書履歴テーブル110aの構成例を示す図である。

**【0091】**

図4に示されるようにサーバ証明書履歴テーブル110aは、この通信システム1において現在有効なサーバ証明書75におけるサーバの名前1101、サーバ証明書のシリアル1102及び有効期限1103をそれぞれ格納するフィールドと、複数のレコードとからなる。

**【0092】**

このように構成されたサーバ証明書履歴テーブル110aを用いると、サーバの名前1101でサーバ証明書75を保持するアプリケーションサーバ30a～30kを特定したり、シリアル1102で現在有効なサーバ証明書75のシリアルの最小値（Se min、図示例では「0x0011」）やシリアルの最大値（Se max、図示例では「0x0110」）を特定したり、有効期限の到来によるサーバ証明書の失効等を管理したりすることができる。

**【0093】**

サーバ証明書期限検索部111は、定期的にサーバ証明書履歴蓄積部110に蓄積されているサーバ証明書履歴テーブル110aの有効期限を参照し、有効期限が1月以内に迫ったサーバ証明書75を検索する。具体的には、サーバ証明書期限検索部111は、時計104から現在時刻を読み取り、現在時刻から1ヶ月後までの間に有効期限が切れるサーバ証明書75を検索する。そしてもし現在時刻から1ヵ月後までの間に有効期限が切れるサーバ証明書75が存在すれば、その有効期限が迫ったサーバ証明書75のシリアル（例えば、図4において針ウド映画と大波ゲームの有効期限が1月以内に迫っている場合には、大きな値を有する大波ゲームのシリアル「0x0012」）を実際に失効させるべきシリアルとして失効証明書検索部113に通知する。

**【0094】**

サーバ証明書失効通知部112は、失効させるサーバ証明書75のシリアルの入力を受け付けて、そのシリアルを失効証明書検索部113に通知する。すなわ

ち、認証局では、アプリケーションサーバのサーバ証明書 75 の安全性を常にチェックしており、次の (1) ～ (3) の場合等に、認証局はサーバ証明書失効通知部 112 から失効させるサーバ証明書 75 のシリアル（例えば、図 4 においてロボット調教師のサーバ証明書 75 を失効させる場合には、ロボット調教師のシリアル「0x0049」）を実際に失効させるべきシリアルとしてサーバ証明書失効通知部 112 から入力し、サーバ証明書 75 の失効を行う。

- (1) アプリケーションサーバのサーバ秘密鍵が暴露された
- (2) アプリケーションサーバの運用を停止した
- (3) アプリケーションサーバの名前を変更した

#### 【0095】

失効証明書検索部 113 は、サーバ証明書期限検索部 111 あるいはサーバ証明書失効通知部 112 から通知された失効させるべきシリアルと同じか、それより小さいシリアルをサーバ証明書履歴テーブル 110a の中すべて列挙し、証明書失効通知部 114 にその名前をすべて通知する。そして、失効証明書検索部 113 は、列挙したシリアルに対してサーバ証明書 75 の更新がすべて終了した後に、失効させるべきシリアルの最大値に「1」加えたものに失効番号を更新し、失効番号蓄積部 115 に蓄積する。また、失効証明書検索部 113 は、列挙したシリアルに対してサーバ証明書 75 の更新がすべて終了した後に、サーバ証明書履歴蓄積部 110 から列挙したシリアルのサーバ証明書 75 に関する情報を削除する。

#### 【0096】

証明書失効通知部 114 は、失効証明書検索部 113 から通知された名前のアプリケーションサーバ 30a～30k に対してサーバ証明書 75 の更新要求を行う。アプリケーションサーバ 30a～30k はサーバ証明書 75 の更新要求に従ってサーバ証明書 75 を更新する。この際、サーバ証明書送信部 109 は、更新されたサーバ証明書 75 の送信を失効証明書検索部 113 に通知する。

#### 【0097】

失効番号蓄積部 115 は、サーバ証明書送信部 109 から発行されたサーバ証明書 75 のシリアルの内、現在も有効な最も小さいシリアルを失効番号として蓄

積する。なお、失効番号の初期値は「0」である。失効番号蓄積部115に蓄積された失効番号は、失効情報署名部116に送られる。

#### 【0098】

失効情報署名部116は、失効情報90に必要な発行者91と、失効番号92と、署名93とで失効情報90を組み立てて、失効情報通知部117に出力する。なお、署名93は、ここでは発行者91及び失効番号92を連結したものをCA秘密鍵蓄積部103に蓄積されたCA秘密鍵で暗号化することで作成されている。

#### 【0099】

失効情報通知部117は、失効情報90をリポジトリ20に通知する。

リポジトリ20は、失効情報蓄積部201と、通信部202とを備える。

#### 【0100】

リポジトリ20の失効情報蓄積部201は、サーバ証明書作成装置10から失効情報90が送信されてくると、送信されてきた失効情報90を失効情報蓄積部201に蓄積する。

#### 【0101】

通信部202は、上述の暗号なしのプロトコル等に従ってインターネット50を介して端末40a～40nと通信するインターフェースであり、端末40a～40nから失効情報90配信のリクエストがあった場合、失効情報蓄積部201に蓄積されている失効情報90をリクエストを発した端末40a～40nに送信する。このとき、通信は暗号化する必要はなく、またリポジトリのサーバ認証も必要がない。

#### 【0102】

アプリケーションサーバ30a～30kは、鍵ペア作成部301と、CSR作成部302と、サーバ秘密鍵蓄積部303と、サーバ証明書蓄積部304と、アプリサーバ部305と、通信部306とを備える。

#### 【0103】

鍵ペア作成部301は、アプリケーションサーバ30a～30k設置時に、RSA暗号で暗号及び復号する時の鍵ペアであるサーバ公開鍵とサーバ秘密鍵を作

成する。

【0104】

C S R作成部302は、認証局に対してサーバ証明書75を作成させる時の雛形、すなわちサーバ公開鍵とサーバの名前を含むC S R70を作成し、サーバ証明書作成装置10に送付する。

【0105】

サーバ秘密鍵蓄積部303は、鍵ペア作成部301が作成したサーバ秘密鍵を蓄積する。

【0106】

サーバ証明書蓄積部304は、サーバ証明書作成装置10から受信したサーバ証明書75を蓄積する。

【0107】

なお、サーバ証明書作成装置10からサーバ証明書75の更新要求があった場合には、鍵ペア作成部301は新しいサーバ公開鍵及びサーバ秘密鍵を作成し、設置時と同様にC S R作成部302は新しいサーバ公開鍵でC S R70を作成しサーバ証明書作成装置10にサーバ証明書75の作成を依頼し、サーバ証明書蓄積部304は新しいサーバ証明書75をサーバ証明書作成装置10から受け取り蓄積する。

【0108】

アプリサーバ部305は、通信部306を介して受信したリクエストを処理してレスポンスを作成し、作成したレスポンスを通信部306に出力する。

【0109】

通信部306は、上述の暗号化のためのプロトコル等に従ってインターネット50を介して端末40a～40nと通信するインターフェースであり、端末40a～40nから送信されてきたリクエストやコマンドを解析したり、その結果に応じてサーバ認証のためにサーバ証明書75をサーバ証明書蓄積部304から取り出し端末40a～40nに送信したり、端末40a～40nから受信した暗号の種類をサーバ秘密鍵蓄積部303に蓄積したサーバ秘密鍵で復号し、暗号化通信の共有鍵を作成したり、端末40a～40nから暗号化した通信でリクエスト

を受けた場合、リクエストを復号してアプリサーバ部 305 に出力したり、アプリサーバ部 305 から依頼されたレスポンスを暗号化して端末 40a ~ 40n に出力したりする。

#### 【0110】

端末 40a ~ 40n は、アプリケーションサーバ 30a ~ 30k に対するリクエストを出力した、アプリケーションサーバ 30a ~ 30k からのレスポンスを受信するアプリケーション部 410 と、通信部 420 と、上記リクエスト及びレスポンスの送受信の前にアプリケーションサーバ 30a ~ 30k から送られてくるサーバ証明書 75 を検証するサーバ証明書検証部 430 とを備える。

#### 【0111】

通信部 420 は、上述の暗号化あるいは非暗号のプロトコル等に従ってインターネット 50 を介してアプリケーションサーバ 30a ~ 30k やリポジトリ 20 と通信したりするインターフェースであり、アプリケーションサーバ 30a ~ 30k から送信されてきたコマンドを解析したり、その結果に応じてサーバ証明書検証部 430 に処理を依頼したり、アプリケーション部 410 やサーバ証明書検証部 430 から渡されたデータをアプリケーションサーバ 30a ~ 30k に送信したり、サーバ証明書検証部 430 から渡されたデータをリポジトリ 20 に送信したり、リポジトリ 20 から失効情報 90 を受信したりする。

#### 【0112】

具体的には、通信部 420 は、通信部 306 に対して暗号化通信の開始を要求する。また、通信部 420 は、通信部 306 からサーバ証明書 75 を受信し、受信したサーバ証明書 75 をサーバ証明書検証部 430 に出力する。そして通信部 420 は、サーバ証明書検証部 430 からサーバ証明書 75 の異常や失効を通知された場合、サーバ証明書 75 の異常を通信部 306 に通知して通信を切断し、エラーをアプリケーション部 410 に通知する。また、通信部 420 は、サーバ証明書 75 の署名が正常であり、かつ、サーバ証明書 75 が失効されていないときは、プリマスタシークレットを作成し、サーバ証明書 75 に含まれるサーバ公開鍵を用いてプリマスタシークレットを暗号化して通信部 306 に送信する。また通信部 420 は、それまでの得たデータから暗号化通信の暗号鍵を作成する

。そして以降の通信において暗号鍵を用いた暗号化通信を行う。さらに、通信部 420 は、リポジトリ 20 の通信部 202 に失効情報 90 の配信を要求し、リポジトリ 20 から受信した失効情報 90 を署名検証部 434 に出力する。

#### 【0113】

サーバ証明書検証部 430 は、失効情報要求部 431 と、署名検証部 432 と、CA 証明書蓄積部 433 と、署名検証部 434 と、失効番号検証部 435 と、失効番号蓄積部 436 と、証明書シリアル抽出部 437 と、失効判定部 438 等とからなる。

#### 【0114】

失効情報要求部 431 は、定期的によりポジトリ 20 から失効情報 90 を取得するよう通信部 420 に要求する。

#### 【0115】

署名検証部 432 は、通信部 420 からサーバ証明書 75 を受信すると、CA 証明書蓄積部 433 から CA 公開鍵を取り出し、サーバ証明書 75 の署名を検証し、署名が異常であれば通信部 420 に異常を通知する。

#### 【0116】

CA 証明書蓄積部 433 は、サーバ証明書作成装置 10 から入手した CA 証明書 60 を、予め蓄積する。

#### 【0117】

署名検証部 434 は、通信部 420 から失効情報 90 を受信すると、CA 証明書蓄積部 433 から CA 公開鍵を取り出し、失効情報 90 の署名の検証を行い、署名が正しければ失効番号を失効番号検証部 435 に出力する。

#### 【0118】

失効番号検証部 435 は、失効番号蓄積部 436 から現在の失効番号を呼び出し、署名検証部 434 から入力された失効番号が現在の失効番号より大きい場合に限って入力された失効番号を新しい失効番号として失効番号蓄積部 436 に蓄積する。

#### 【0119】

失効番号蓄積部 436 は、失効番号の初期値として「0」を予め記憶しており

、失効番号検証部 435 から失効番号が出力されるごとにその時点の最新の失効番号を更新しつつ蓄積する。

#### 【0120】

証明書シリアル抽出部 437 は、入力されたサーバ証明書 75 からシリアルを抽出し、失効判定部 438 に出力する。

#### 【0121】

失効判定部 438 は、失効番号蓄積部 436 から失効番号を取り出し、抽出したシリアルと比較する。失効判定部 438 は抽出したシリアルが失効番号より小さい場合は、失効判定部 438 は、サーバ証明書 75 が失効していることを通信部 420 に通知する。

#### 【0122】

次いで、サーバ証明書作成装置 10、アプリケーションサーバ 30a～30k 及び端末 40a～40n の動作を詳述する。

#### 【0123】

図 5 は、サーバ証明書組立部 107 が行う証明書用シリアル設定処理の動作を示すフローチャートである。

#### 【0124】

サーバ証明書組立部 107 は、まずサーバ証明書 75 に設定すべきシリアル S<sub>e</sub> の初期値として「0」を設定し (S11)、CSR 受信部 106 を介して CSR 70 を受信するのを待つ (S12)。CSR 70 を受信すると (S12 で Yes)、サーバ証明書組立部 107 は、シリアル蓄積部 105 からシリアル S<sub>e</sub> を読み取り (S13)、時計 104 から読み取った現在時刻や CSR 70 等を用いてサーバ証明書を組み立て (S14)、組み立てたサーバ証明書を署名部 108 に出力した後、シリアル蓄積部 105 に蓄積させるシリアル S<sub>e</sub> を「1」インクリメントし (S15)、サーバ証明書の要部、名前、シリアル、有効期限をサーバ証明書履歴テーブル 110a に蓄積させる (S16)。このような処理 (S12～S16) を繰り返すことにより、シリアルが単調増加するサーバ証明書 75 が順次発行されることになる。

#### 【0125】



次いでサーバ証明書期限検索部 111 が行う証明書期限管理処理を説明する。

#### 【0126】

図 6 は、サーバ証明書期限検索部 111 が行う証明書期限管理処理の動作を示すフローチャートである。なお、この処理は、所定の時間ごとに定期的に行われる。

#### 【0127】

サーバ証明書期限検索部 111 は、まずサーバ証明書履歴テーブル 110 a のシリアルをサーチし、サーバ証明書履歴テーブル 110 a に格納されているシリアルの最小値  $S_{emin}$  及びシリアルの最大値  $S_{emax}$  を取得し、有効期限の到来が早いシリアル、すなわちシリアルの最小値  $S_{emin}$  をセットする (S21)。そして、サーバ証明書期限検索部 111 は、そのシリアルについて 1 月以内に有効期限が到来するか否か判断する (S22)。判断の結果到来する場合には (S22 で Yes)、サーバ証明書期限検索部 111 は、そのシリアルを実際に失効させるべきシリアルの最大値  $S_{eend}$  にセットし、次のレコードの有効期限をサーチするためにシリアル  $S_e$  を「1」インクリメントする (S23)。シリアル  $S_e$  のインクリメントが終わると、サーバ証明書期限検索部 111 は、サーバ証明書履歴テーブル 110 a の最後のレコードのシリアル  $S_{emax}$  まですべて有効期限の到来をみたか判断する (S24)。最後のレコードまでみていなければ (S24 で No)、サーバ証明書期限検索部 111 は、ステップ S22 ~ S24 を繰り返し実行し、実際に失効させるべきシリアルの最大値  $S_{eend}$  を順次取得する。

#### 【0128】

判断の結果 1 月以内に有効期限が到来しない場合 (S22 で No)、あるいは最後のレコードまでみた場合 (S24 で Yes) には、サーバ証明書期限検索部 111 は、実際に失効させるべきシリアルの最大値  $S_{eend}$  を失効証明書検索部 113 に通知する (S25)。

#### 【0129】

このような処理を繰り返すことにより有効期限が到来するサーバ証明書 75 のシリアルが時々刻々失効証明書検索部 113 に通知される。

## 【0130】

次いで、失効証明書検索部113が行う有効期限到来による失効証明書検索処理を説明する。

## 【0131】

図7は、失効証明書検索部113が有効期限到来による失効証明書検索処理の動作を示すフローチャートである。なお、この処理は、所定の時間ごとに定期的に行われる。

## 【0132】

失効証明書検索部113は、サーバ証明書期限検索部111から実際に失効させるべきシリアルの最大値 *Seend* の通知がくるのを待つ (S31)。実際に失効させるべきシリアル of 最大値 *Seend* の通知がくると (S31で *Yes*)、失効証明書検索部113は、サーバ証明書履歴テーブル110aの最小のシリアル *Semin* からこのシリアル of 最大値 *Seend* までのシリアルに対応するサーバの名前を証明書失効通知部114に通知する (S32)。これにより、証明書失効通知部114から各アプリケーションサーバ30a～30kに失効通知80が送られ、この失効通知80を受けたアプリケーションサーバ30a～30kがCSR70を送信し、これらのアプリケーションサーバ30a～30kに単調に増加するシリアルが付されたサーバ証明書75が順次新たに発行されることになる。

## 【0133】

そして、失効証明書検索部113は、シリアル of 値が増加された新たなサーバ証明書が全て発行されるのを待つ (S33)。

## 【0134】

サーバ証明書75を発行し終わると (S33で *Yes*)、失効証明書検索部113は、シリアル *Semin*～*Seend* のレコードを全て削除し (S34)、実際に失効させるべきシリアル of 最大値 *Seend* に「1」加えた値を失効シリアルとして失効番号蓄積部115に格納する (S32)。

## 【0135】

このような処理を繰り返すことにより、有効期限を迎えるサーバ証明書75は

順次失効の対処とされ、この失効の対象とされたサーバ証明書 75 を有するアプリケーションサーバ 30 a ~ 30 k はシリアル番号が増加された新たなサーバ証明書 75 に更新することになる。

#### 【0136】

次いで、失効証明書検索部 113 が行うサーバ証明書失効通知部 112 からの失効通知による失効検索処理を説明する。

#### 【0137】

図 8 は、失効証明書検索部 113 が行う失効通知による失効証明書検索処理の動作を示すフローチャートである。なお、この処理は、所定の時間ごとに定期的に行われる。

#### 【0138】

失効証明書検索部 113 は、サーバ証明書失効通知部 112 から失効通知がくるのを待つ (S41)。失効通知があると、失効証明書検索部 113 は、通知されたシリアル  $S_e$  を特定し (S42)、サーバ証明書履歴テーブル 110 a の最小のシリアル  $S_{emin}$  からこの特定されたシリアル  $S_e$  までのシリアルに対応するサーバの名前を証明書失効通知部 114 に通知する (S43)。これにより、証明書失効通知部 114 から各アプリケーションサーバ 30 a ~ 30 k に失効通知 80 が送られ、この失効通知 80 を受けたアプリケーションサーバ 30 a ~ 30 k が CSR 70 を送信し、これらのアプリケーションサーバ 30 a ~ 30 k に単調に増加するシリアルが付されたサーバ証明書 75 が順次新たに発行されることになる。

#### 【0139】

そして、失効証明書検索部 113 は、新たにサーバ証明書が全て発行されるのを待つ (S44)。

#### 【0140】

サーバ証明書 75 を発行し終わると (S44 で Yes)、失効証明書検索部 113 は、シリアル  $S_{emin}$  ~ 特定したシリアル  $S_e$  のレコードを全て削除し (S45)、実際に失効させるべき特定されたシリアル  $S_e$  に「1」加えた値を失効シリアルとして失効番号蓄積部 115 に格納する (S46)。

## 【0141】

このような処理を繰り返すことにより、失効の対象とされたサーバ証明書75のみならずこれより小さな値のシリアルが付されたサーバ証明書75は全て失効の対処とされ、この失効の対象とされたサーバ証明書75を有するアプリケーションサーバ30a～30kはシリアル番号が増加された新たなサーバ証明書75に更新することになる。

## 【0142】

次いで、失効情報署名部116が行う失効情報組立処理を説明する。

## 【0143】

図9は、失効情報署名部116が行う失効情報組立処理の動作を示すフローチャートである。

## 【0144】

失効情報署名部116は、失効番号蓄積部115から失効シリアルS<sub>e</sub>の初期値「0」をセットする(S51)。そして、この失効シリアルS<sub>e</sub>と、予め保持している発行者と、CA秘密鍵蓄積部103から読み出したCA秘密鍵を用いて形成する署名とで失効情報90を組み立てて、失効情報通知部117に出力する。

## 【0145】

次いで、失効情報署名部116は、失効番号蓄積部115をモニタし、失効シリアルが失効シリアル変化するのをまつ(S52)。ここで、失効シリアルから「1」減算した値のシリアル以下のサーバ証明書75は全て失効の対象とされている。このため、このステップS52での実際の判断は、失効シリアルが増加したか否かの判断でたりる。失効シリアルが増加すると、失効情報署名部116は、変化後の失効シリアルS<sub>e</sub>を失効番号蓄積部115から読み取り(S53)、この失効シリアルS<sub>e</sub>と、予め保持している発行者と、CA秘密鍵蓄積部103から読み出したCA秘密鍵を用いて形成する署名とで失効情報90を組み立てて(S54)、失効情報通知部117に出力する。

## 【0146】

このような処理を繰り返すことにより、リポジトリ20の失効情報蓄積部20

1 には、失効シリアル値が増加する失効情報 9 0 が順次蓄積されることになる。

#### 【0 1 4 7】

次いで、端末 4 0 a ~ 4 0 n のサーバ証明書検証部 4 3 0 が行う失効情報取得処理を説明する。

#### 【0 1 4 8】

図 1 0 は、サーバ証明書検証部 4 3 0 の各部が行う失効情報取得処理の動作を示すフローチャートである。なお、この処理は、所定の時間（1 月に 1 回）ごとに定期的に行われる。

#### 【0 1 4 9】

各端末 4 0 a ~ 4 0 n の失効情報要求部 4 3 1 は、まず、リポジトリ 2 0 から失効情報 9 0 を定期的（1 月に 1 回）に入手して、失効番号を蓄積する。具体的には、失効情報要求部 4 3 1 は、内部タイマーによる計時で 1 月経過するのを待ち（S 6 1）、1 月経過すると（S 6 1 で Y e s）、リポジトリ 2 0 に対して失効情報の配信を要求し（S 6 2）、失効情報 9 0 が配信されるのを待つ（S 6 3）。

#### 【0 1 5 0】

このとき、入手した失効情報 9 0 が偽である場合の失効番号を蓄積すると、正規のアプリケーションサーバを不正であると判断したり、不正なアプリケーションサーバを正規とみなしたりするので、次のチェックを行う。

#### 【0 1 5 1】

すなわち、失効情報 9 0 が送られてくると（S 6 2 で Y e s）、まず最初に署名検証部 4 3 4 は、失効情報 9 0 の署名が正しいかを確認する（S 6 4）。失効情報 9 0 の署名はサーバ証明書作成装置 1 0 しか行えないため、署名が正しいければそれは正しいデータとする。

#### 【0 1 5 2】

次に、失効番号が現在蓄積しているより大きな番号であることを確認する。具体的には、失効番号検証部 4 3 5 は、配信された失効シリアルを取得し（S 6 5）、配信された失効シリアル値が失効番号蓄積部 4 3 6 に蓄積している失効シ

リアル値より大きいか否かを判断する(S66)。失効番号は、サーバ証明書75の失効により単調増加され、減少することがない。

#### 【0153】

したがって、受信した失効情報90の失効番号が現在保持している失効番号より大きい番号であれば(S66でYes)、配信された失効シリアルを蓄積する(S67)。これに対してし、現在の失効番号より小さな番号であれば(S66でNo)、それは偽の失効番号であるか、なにかの手違いであると推定し、失効情報を廃棄する(S68)。

#### 【0154】

このような処理を繰り返し行うことにより、サーバ証明書検証部430は値が単調に増加する正規の失効番号だけを蓄積することができる。

#### 【0155】

次に端末40a～40n及びアプリケーションサーバ30a～30k間で暗号化して通信を行う場合について説明する。

#### 【0156】

図11は、暗号化して通信を行う場合のシーケンス図である。なおここでは、端末40aとアプリケーションサーバ30aとの間で行われた場合をその代表例として説明する。

#### 【0157】

端末40aのアプリクライアント部410は、暗号化してアプリケーションサーバ30aにリクエスト3を送るよう通信部420に指示を行う(S100)。通信部420は、クライアント乱数と通信部420が処理できる暗号の種類を含んだClientHello packetsをアプリケーションサーバ30aの通信部306に送信し、SSLのハンドシェイクを開始する(S101)。

#### 【0158】

アプリケーションサーバ30aの通信部306は、ClientHello packetsから暗号の種類を決定し、サーバ乱数とセッションIDとともにServerHello packetsで暗号の種類を送り(S102)、サーバ証明書蓄積部304からサーバ証明書75を取り出し(S103)、サーバ証明書75をCe

r t i f i c a t e パケットとしてアプリケーションサーバ 30a の通信部 420 に送信し (S104)、さらに S e r v e r H e l l o D o n e パケットを通信部 420 に送る (S107)。

#### 【0159】

端末 40a の通信部 420 は、C e r t i f i c a t e パケットからサーバ証明書 75 を取り出し、サーバ証明書検証部 430 に送る (S105)。サーバ証明書検証部 430 は、サーバ証明書 75 が不正でないか検証し、検証結果を通信部 306 に通知する (S106)。サーバ証明書 75 が不正であれば、通信部 420 は、アラートパケットを通信部 306 に送信して通信を切断し、アプリケーション部 410 にエラーを返す。これに対して、サーバ証明書 75 が不正でない場合には、通信部 420 は、暗号化の共有鍵を計算するためのプリマスターシークレットを作成し、サーバ証明書 75 に含まれるサーバ公開鍵で暗号化し、S e r v e r H e l l o D o n e パケットの到着後に暗号化されたプリマスターシークレットを含む C l i e n t K e y E x c h a n g e パケットを通信部 306 に送信し (S108)、C h a n g e C i p h e r S p e c パケットを通信部 306 に送信する (S109)。C h a n g e C i p h e r S p e c パケットは暗号化の開始を示すパケットである。通信部 420 は、クライアント乱数とサーバ乱数とプリマスターシークレットから暗号化に使用する共通鍵 A を作成し、ハンドシェークの終了を示す F i n i s h e d パケットを作成した共通鍵 A で暗号化してアプリケーションサーバ 30a の通信部 306 に送信する (S110)。

#### 【0160】

アプリケーションサーバ 30a の通信部 306 は、C l i e n t K e y E x c h a n g e から暗号化されたプリマスターシークレットを取り出し、サーバ秘密鍵を用いてプリマスターシークレットに復号し、サーバ乱数、クライアント乱数とともに暗号化に使用する共通鍵 B を作成する。SSL のハンドシェークが正常に行われた場合、通信部 306 の持つ共通鍵 A と通信部 420 の持つ共通鍵 B は同一となる。通信部 306 は、受信した F i n i s h e d パケットを共通鍵 B で復号し、正常に復号できれば F i n i s h パケットを暗号化して通信部 420 に送付する (S111)。この F i n i s h パケット以降の通信は、すべて暗号化

して行われる。

【0161】

端末40aの通信部420は、受信したFinished packetsを復号し、正常に復号できれば、リクエスト3を暗号化してアプリケーションサーバ30aの通信部306に送付する(S112)。

【0162】

アプリケーションサーバ30aの通信部306は、リクエスト3を復号し、アプリサーバ部305に送る(S113)。アプリサーバ部305は、リクエスト3を処理してレスポンス3を生成し、端末40a~40nに送るよう通信部306に指示する(S114)。通信部306は、端末40aの通信部420にレスポンス3を暗号化して送信する(S115)。

【0163】

端末40aの通信部420は、レスポンス3を復号してアプリケーションクライアント部410に送付する(S116)。

【0164】

以上のように暗号化を行い通信する。

【0165】

次いで、サーバ証明書検証部430が行う検証について説明する。

【0166】

図12は、サーバ証明書検証部430が行うサーバ証明書75の検証動作を示すフローチャートである。

【0167】

サーバ証明書検証部430の署名検証部432は、サーバ証明書75を取得すると、取得したサーバ証明書75から発行者を取り出し、CA証明書蓄積部433から、その発行者のCA証明書60を検索する。そして、CA証明書60からCAの公開鍵を取り出し、CAの公開鍵を用いてサーバ証明書75の署名のチェックをする。具体的には、署名検証部432は、サーバ証明書75が配信されてくるのを待ち(S81)、配信されてくると(S81でYes)、サーバ証明書75の発行者を取得し(S82)、発行者が同一のCA証明書60をCA証明書



蓄積部 433 から検索する (S83)。そして、署名検証部 432 は、検索によって得られた CA 証明書 60 の CA 公開鍵を取り出し (S84)、公開鍵で復号化することによりサーバ証明書の署名が正しいか否か判断する (S85)。

#### 【0168】

チェックの結果、サーバ証明書 75 の署名が不正であれば (S85 で署名 NG)、署名の検証エラーのエラーコードを通信部 420 に通知して (S90)、検証を終了する。これに対して、署名が正しければ (S85 で署名 OK)、証明書シリアル抽出部 437 は、サーバ証明書 75 からシリアル (サーバシリアル) を取り出す (S86)。そして、失効判定部 438 は、失効番号蓄積部 436 から失効番号を取り出し、証明書シリアル抽出部 437 が取り出したシリアルと比較する。すなわち、サーバシリアルと失効シリアルとの大小関係を判断する (S88)。

#### 【0169】

もしシリアルが失効番号より小さければ (S88 で No)、失効判定部 438 は、そのサーバ証明書 75 が失効していると判断し、失効のエラーコードを通信部 420 に通知して (S90)、検証を終了する。これに対して、もしシリアルが失効番号より大きいと同じであれば (S88 で Yes)、失効判定部 438 は、そのサーバ証明書 75 は正しいと判断して、通信部 420 に正常終了を通知する。

#### 【0170】

このような処理により署名が正当で、しかも失効番号以上の値のシリアルを含むサーバ証明書 75 をアプリケーションサーバ 30a が送った場合にだけ認証される。

#### 【0171】

ここで、サーバ証明書作成装置 10 が作成するサーバ証明書 75 のシリアルと失効番号の関係について説明する。

#### 【0172】

図 13 は、サーバが 4 台あったときのサーバ証明書 75 のシリアルと失効番号との関係を示す図である。

## 【0173】

なお、ここでは各サーバをA, B, C, Dとし、サーバはそれぞれ時刻「a」, 「b」, 「c」, 「d」に設置されるものとし、各サーバが保持するサーバ証明書75のシリアルはそれぞれ「0」, 「1」, 「2」, 「3」であるものとして説明する。

## 【0174】

時刻「e」にサーバCのサーバ証明書75の安全性が危惧された場合、この時点におけるサーバ証明書履歴蓄積部110に蓄積されている情報は次のとおりである。

## 【0175】

サーバ名	:	シリアル	:	有効期限
A	:	0	:	$a + 13$ (ヶ月)
B	:	1	:	$b + 13$ (ヶ月)
C	:	2	:	$c + 13$ (ヶ月)
D	:	3	:	$d + 13$ (ヶ月)

したがって、サーバ証明書作成装置10の失効証明書検索部113は、サーバCのサーバ証明書75のシリアル「2」より小さなシリアルをもつサーバ証明書75を検索する。結果はサーバA及びサーバBのサーバ証明書75である。従って、サーバ証明書作成装置10の証明書失効通知部114は、サーバA, B, Cに対してサーバ証明書75の更新要求（サーバ証明書75の失効通知）を行う。その結果サーバA, B, Cから新しいサーバ証明書75の作成要求があり、それぞれシリアルが「4」, 「5」, 「6」であるサーバ証明書75を新規に作成し、各アプリケーションサーバA～Cに返送する。このとき作成したサーバ証明書75の有効期限は $e + 13$ ヶ月とする。また同時にサーバ証明書履歴蓄積部110のデータは

サーバ名	:	シリアル	:	有効期限
D	:	3	:	$d + 13$ (ヶ月)
A	:	4	:	$e + 13$ (ヶ月)
B	:	5	:	$e + 13$ (ヶ月)

C : 6 : e + 13 (ヶ月)

に更新される。

#### 【0176】

サーバ証明書作成装置 10 の失効番号蓄積部 115 は、各サーバのサーバ証明書 75 が更新された後に失効番号をその時点で有効かつ最小のシリアル「3」に変更し、このシリアルを含む失効情報 90 をリポジトリ 20 の失効情報蓄積部 201 に蓄積させる。すなわち、新しい失効番号は、失効原因となったサーバ C の元のサーバ証明書 75 のシリアル「2」に「1」を加えた値である「3」である。

#### 【0177】

端末 40a ~ 40n は、リポジトリ 20 から失効番号を定期的に入手して蓄積する。このとき偽の失効番号を蓄積すると、正規のサーバを不正であると判断したり、不正なサーバを正規にみなしたりするので次のチェックを行う。まず最初に失効情報の署名を確認する。失効情報の署名は CA にしか署名できないため署名が正しければそれは正しいデータとする。次に失効番号が現在蓄積しているより大きな番号であることを確認する。失効番号はサーバ証明書の失効により増加を行うが、減少はしないので現在の失効番号より小さな番号であればそれは偽の失効番号であるか、なにかの手違いであると推定し、それを廃棄する。

#### 【0178】

ところで、サーバ C のサーバ証明書 75 を用いてサーバの成りすましがあったとした場合、なりすましたサーバのサーバ証明書 75 のシリアルは「2」であり、その時点で端末の失効番号は「3」であるため、失効番号より小さなシリアルを持つサーバ証明書 75 は失効されているという条件に合致し、そのサーバを信用することはない。

#### 【0179】

また、サーバ証明書期限検索部 111 は、常にサーバ証明書履歴蓄積部 110 を検索し、現在時刻より 1 ヶ月内に有効期限がくるサーバ証明書 75 を検索する。例えば d + 12 ヶ月を過ぎれば、サーバ D のサーバ証明書 75 の期限が 1 ヶ月内となる。このときサーバ証明書期限検索部 111 は、サーバ D が保持するサー

サーバ証明書 75 のシリアル「3」を失効証明書検索部 113 に通知し、証明書失効通知部 114 はサーバ D に対してサーバ証明書 75 の更新を要求する。またサーバ D のサーバ証明書 75 のシリアルより小さなシリアルを持つサーバ証明書 75 を持つサーバがあれば、そのサーバに対してもサーバ証明書 75 の更新要求を行う。そしてこれらのサーバ証明書 75 の更新が終わったあとで失効番号をサーバ D のサーバ証明書 75 のシリアルに「1」を加えた「4」に更新する。

#### 【0180】

このように有効期限が近づいたサーバ証明書 75 を更新するときに、有効期限の近づいたサーバ証明書 75 が持つシリアルより小さいシリアルをもつサーバ証明書 75 を全て更新し、期限の近づいたサーバ証明書 75 のシリアルに「1」加えたものをあらたな失効番号とすることにより、有効期限が切れたサーバ証明書 75 によってサーバが成りすまされた場合でも、時計がなく期限が正確に判断できない機器でも失効番号によってそのサーバ証明書 75 の失効を確認できる。

#### 【0181】

なお、ここでは更新後のシリアルをサーバ A, B, C の順で「4」, 「5」, 「6」としたが、特にこの順でなくともよい。

#### 【0182】

なお、本実施の形態 1 では、シリアルの初期値を「0」とし、サーバ証明書 75 の発行毎に「1」増加させたが、初期値は自由に設定でき、増加する値も単調増加する範囲において発行毎に異なってもよい。

#### 【0183】

また、本実施の形態 1 では、失効番号の初期値を「0」としたが、シリアルの初期値以下の小さい値であれば、なんでもよい。つまり、例えばサーバ証明書 75 のシリアルの初期値を「1」とした場合、失効番号の初期値を「0」としてもよく、「1」としてもよい。

#### 【0184】

また、サーバ証明書 75 のシリアルの初期値が失効番号の初期値以上の値に設定された状態で単調増加するシリアルのサーバ証明書 75 が発行されるので、失効シリアルを参照したのと同等の機能が確保されるため、この実施の形態では参

照しなかったが、失効番号を実際に参照して失効番号以上のシリアルサーバ証明書75を発行するようにしてもよい。

#### 【0185】

以上のように、本実施の形態1によれば、有効期限が切れそうなサーバ証明書を保持するアプリケーションサーバに対して失効通知を送り、新たなサーバ証明書を発行し、もとのサーバ証明書を失効させて使えなくなるようにしている。したがって、端末40a～40nは、有効期間をチェックする必要がなく、正確な時計を持つ必要もなくなる。また、失効情報90には1つの失効シリアルだけが記録され、端末40a～40nはこれを記憶し、サーバ証明書75のシリアルと失効番号との大小関係でサーバ証明書75の有効性を判断するので、従来のようなりソースを用意する必要もなく、簡なりソースでたり、ネット家電等にも適用できる。

#### 【0186】

(実施の形態2)

以下、本発明の実施の形態2に係る通信システムについて説明する。

#### 【0187】

図14は、本発明の実施の形態2に係る通信システム2の全体構成を示すブロック図である。なお、図1に示される通信システム1の構成と同じ構成部分に同じ番号を付し、その説明を省略する。

#### 【0188】

この通信システム2は、実施の形態1の通信システム1と同様、認証局が使用するサーバ証明書作成装置11及びリポジトリ21と、映像コンテンツなどのアプリケーション提供者が使用する複数のアプリケーションサーバ30a～30kと、ユーザが使用する複数の端末41a～41nと、リポジトリ21、アプリケーションサーバ30a～30k及び端末41a～41nを接続するインターネット50とから構成される。

#### 【0189】

ところで、実施の形態1の通信システム1は、サーバ証明書作成装置10からリポジトリ20に失効情報90を送信し、リポジトリ20から端末40a～40

nに失効情報90を送信するように構成されている。これに対して実施の形態2の通信システム2は、サーバ証明書作成装置11からリポジトリ21には失効番号だけで構成される失効情報90bを送信するように構成されており、この点が通信システム1の構成と大きく異なっている。

#### 【0190】

また、通信システム1では、リポジトリ20から各端末40a～40nに失効情報90を暗号なしで送信し、各端末において失効情報90の署名でその失効情報のすり替えをチェックするように構成されている。これに対して通信システム2は、リポジトリ21がは、サーバ証明書作成装置11からリポジトリ21にサーバ証明書75を発行し、リポジトリ21は、端末41a～41nから失効番号配信の要求がくると、アプリケーションサーバ30a～30kの場合と同様、サーバ証明書75を送信し、端末40a～40nからサーバ認証を受け、SSLによるセッション鍵を共有した後、失効番号を暗号化して配信するように構成されており、この点が通信システム1の構成と大きく異なっている。

#### 【0191】

このため、サーバ証明書作成装置11は、アプリケーションサーバ30a～30kの場合と同様、鍵ペア作成部101、CA証明書作成部102、CA秘密鍵蓄積部103、時計104、シリアル蓄積部105、CSR受信部106、サーバ証明書組立部107、署名部108、サーバ証明書送信部109、サーバ証明書履歴蓄積部110、サーバ証明書期限検索部111、サーバ証明書失効通知部112、失効証明書検索部113、証明書失効通知部114を備え、リポジトリ21から送られてきたCSR70を受け付けて、リポジトリ21にサーバ証明書75を発行したり、このサーバ証明書75が失効の対象となった場合にリポジトリ21に失効通知80を送信したりするように構成されている。しかも、サーバ証明書作成装置11は、サーバ証明書作成装置10で用いられていた失効情報署名部116が削除され、失効番号蓄積部115に代えて失効番号蓄積部121を、失効情報通知部117に代えて失効番号通知部122を備えて構成される。この失効番号蓄積部121は失効番号蓄積部115と同様に、サーバ証明書送信部109から発行されたサーバ証明書75のシリアルの内、現在も有効な最も小さ

いシリアルを失効番号として蓄積する。なお、失効番号の初期値は「0」である。失効番号通知部122に蓄積された失効番号は、失効情報署名部116に送られる。失効番号通知部122は、失効番号蓄積部121に蓄積されている署名なしの失効番号だけを失効情報90bとしてリポジトリ21に通知する。

#### 【0192】

リポジトリ21は、鍵ペア作成部203と、CSR70作成部204と、サーバ秘密鍵蓄積部205と、サーバ証明書蓄積部207と、失効情報蓄積部208と、通信部209とを備える。

#### 【0193】

リポジトリ21は、アプリケーションサーバ30a～30kと同様に、端末41a～41nとの通信をSSLを用いて行う。このため、鍵ペア作成部203は、設置時やサーバ証明書作成装置11から失効通知80を受信するごとに、サーバ公開鍵とサーバ秘密鍵を新たに作成する。サーバ公開鍵はCSR70作成部204に送られ、サーバ秘密鍵はサーバ秘密鍵蓄積部205に蓄積される。

#### 【0194】

CSR70作成部204は、サーバ公開鍵と予め保持するサーバの名前からCSR70を作成し、サーバ証明書作成装置11に送信する。これによって、サーバ証明書作成装置11は、受信したCSR70からサーバ証明書75を作成し、作成したサーバ証明書75をリポジトリ21に送信する。サーバ証明書蓄積部207は、サーバ証明書75を受信するごとに、受信した新しいサーバ証明書75を蓄積する。

#### 【0195】

失効情報蓄積部208は、サーバ証明書作成装置11から失効番号だけで構成された失効情報90bを受信するごとに、新しい失効番号を蓄積する。

#### 【0196】

通信部209は、上述の暗号化のためのプロトコル等に従ってインターネット50を介して端末41a～41nと通信するインターフェースである。具体的には、通信部209は、端末41a～41nから通信の開始要求を受けたとき、通信部306と同様、サーバ認証のためにサーバ証明書75をサーバ証明書蓄積部

207から取り出し、端末41a～41nに送る。また通信部209は、端末41a～41nから受信した暗号の種類をサーバ秘密鍵蓄積部205に蓄積したサーバ秘密鍵で復号し、暗号化通信の共有鍵を作成する。その後通信部209は、端末41a～41nから暗号化した通信で失効番号のリクエストを受けた場合、失効情報蓄積部208から失効情報90bを取り出し、失効情報90bを暗号化して端末41a～41nに出力する。これに対して、暗号化しない通信でリクエストを受けた場合、通信部209は、通信を切断する。

#### 【0197】

端末41a～41nは、アプリケーション部410と、通信部420に代えて用いられる通信部440と、サーバ証明書検証部430に代えて用いられるサーバ証明書検証部450とから構成される。サーバ証明書検証部450は、サーバ証明書検証部430と同様、署名検証部432、CA証明書蓄積部433、失効番号蓄積部436、失効判定部438を備えるほか、失効情報要求部431に代えて用いられる失効情報要求部451と、証明書シリアル抽出部437に代えて用いられる証明書シリアル抽出部452と、失効番号検証部435に代えて用いられる失効番号検証部453とから構成される。

#### 【0198】

端末41a～41nの失効情報要求部451は、定期的（例えば、1月に1回）にリポジトリ21から失効番号を取得するよう通信部440に要求する。

#### 【0199】

署名検証部432は、CA証明書蓄積部433からCA証明書60を取り出し、サーバ証明書75の署名を検証し、署名が異常であれば通信部440に異常を通知する。

#### 【0200】

証明書シリアル抽出部452は、入力されたサーバ証明書75からシリアルを抽出し、抽出したシリアルを失効判定部438と失効番号検証部453に出力する。

#### 【0201】

失効番号検証部453は、失効番号蓄積部436に蓄積されている失効番号を



取り出し、リポジトリ 2 1 から取得したシリアル（失効番号）と比較したり、証明書シリアル抽出部 4 5 2 から出力されたシリアルと比較する。そして、リポジトリ 2 1 から取得したシリアルが失効番号蓄積部 4 3 6 に蓄積されている失効番号より小さい場合は、失効番号検証部 4 5 3 は、何らかの原因で異常であることを通信部 4 4 0 に通知する。また、失効番号検証部 4 5 3 は、アプリケーションサーバ 3 0 a ～ 3 0 k やリポジトリ 2 1 から抽出したサーバ証明書 7 5 のシリアルが失効番号より小さい場合は、サーバ証明書 7 5 が失効していることを通信部 4 4 0 に通知する。

#### 【0 2 0 2】

通信部 4 4 0 は、上述の暗号化あるいは非暗号のプロトコル等に従ってインターネット 5 0 を介してアプリケーションサーバ 3 0 a ～ 3 0 k やリポジトリ 2 1 と通信したりするインターフェースであり、通信部 4 2 0 と同様にアプリケーションサーバ 3 0 a ～ 3 0 k と通信するほか、リポジトリ 2 1 から送信されてきたコマンドを解析したり、その結果に応じてサーバ証明書検証部 4 3 0 に処理を依頼したり、アプリケーションクライアント部 4 1 0 やサーバ証明書検証部 4 5 0 から渡されたデータをリポジトリ 2 1 に送信したり、リポジトリ 2 1 からサーバ証明書 7 5 及び失効情報 9 0 を受信したりする。つまり、通信部 4 4 0 は、図 1 1 に示される通信プロトコルを用いて失効情報 9 0 b を暗号化通信する。

#### 【0 2 0 3】

具体的には、通信部 4 4 0 は、失効情報要求部 4 5 1 からの失効情報 9 0 b の要求があると、リポジトリ 2 1 の通信部 2 0 9 に対して暗号化通信の開始を要求する。これにより、通信部 4 4 0 には、リポジトリ 2 1 の通信部 2 0 9 よりサーバ証明書 7 5 が通知される。

#### 【0 2 0 4】

通信部 4 4 0 は、受信したサーバ証明書 7 5 を、署名検証部 4 3 2 と、証明書シリアル抽出部 4 5 2 に出力する。この出力の結果署名検証部 4 3 2 から異常を通知された場合、通信部 4 4 0 は、サーバ証明書 7 5 の異常をリポジトリ 2 1 の通信部 2 0 9 に通知して通信を切断する。

#### 【0 2 0 5】

サーバ証明書 75 の署名が正常であり、サーバ証明書 75 が失効されていないときは、通信部 440 は、プリマスタシークレットを作成し、サーバ証明書 75 に含まれるサーバ公開鍵を用いてプリマスタシークレットを暗号化してリポジトリ 21 の通信部 209 に送信する。そして、通信部 440 は、それまでに得たデータから暗号化通信の暗号鍵を作成する。そして以降の通信において暗号鍵を用いた暗号化通信を行う。つまり、通信部 440 は、失効番号のリクエストをリポジトリ 21 に暗号化して送信する。リポジトリ 21 から暗号化された失効情報 90b (失効番号) を受信すると、通信部 440 は、受信した暗号化された失効番号を復号し、失効番号検証部 453 に出力する。

#### 【0206】

失効番号検証部 453 は、失効番号蓄積部 436 から現在の失効番号を読み出し、リポジトリ 21 から通知された失効番号と比較する。このとき現在の失効番号より通知された失効番号が小さければ通知された失効番号は無効と判断し、処理を終了する。なぜならば、失効番号は単調増加するので、現在の失効番号より小さな失効番号に変更されることはありえないからである。また、現在の失効番号と通知された失効番号が同じ場合には、変更がなかったとして処理を終了する。現在の失効番号より通知された失効番号が大きい場合には、失効番号検証部 453 は、通知された失効番号と証明書シリアル抽出部 452 から入力されるリポジトリ 21 のシリアルを比較する。失効番号検証部 453 は、通知された失効番号がリポジトリ 21 のシリアルより小さければ通知された失効番号は無効と判断し処理を終了する。なぜならば、通知された失効番号を有効と仮定すれば、リポジトリ 21 のシリアルが無効、すなわちサーバ証明書 75 が失効しているということになり、無効なサーバ証明書 75 を持つリポジトリ 21 から取得した失効番号が信用できないためである。失効番号検証部 453 は、通知された失効番号がリポジトリ 21 のシリアルより大きい場合であれば、通知された失効番号を新たな失効番号として失効番号蓄積部 436 に蓄積する。

#### 【0207】

なお、失効番号に対する攻撃として、失効番号を小さくして過去に脆弱となったサーバ証明書 75 を有効にする攻撃と、失効番号を大きくしてオーバフローさ

せる攻撃が考えられるが、これらに対するために以上のような失効番号の有効性の判定を行う。

#### 【0208】

以上のようにすることで、失効情報90bの入手の際に署名のチェックを行わなくてもよく、正常な失効番号だけを保持することができる。

#### 【0209】

なお、本発明の他の実施の形態として、発明の構成を、以下のようにしてもよい。

#### 【0210】

証明書発行装置は、失効番号を蓄積する失効番号蓄積手段と、過去に発行したサーバ証明書の識別番号と期限と発行先を蓄積するサーバ証明書情報蓄積手段と、新たにサーバ証明書を発行する証明書発行手段を持ち、新たにサーバ証明書を発行する場合には失効番号蓄積手段に蓄積された失効番号と同じかより大きな識別番号を持つサーバ証明書を発行することを特徴としてもよい。

#### 【0211】

また、証明書発行装置は、サーバ証明書を失効させるときに、サーバ証明書の識別番号を取得し、新たな失効番号として識別番号より大きな番号を失効番号として決定し、失効番号蓄積手段に蓄積し、サーバ証明書情報蓄積手段を検索し、サーバ証明書の識別番号と同じかより小さな識別番号を持つサーバ証明書（以下更新対象サーバ証明書）を取り出し、更新対象サーバ証明書を持つサーバに対して新たな失効番号と同じかより大きな識別番号を持つサーバ証明書に更新する構成としてもよい。

#### 【0212】

また、証明書発行装置は、サーバ証明書情報蓄積手段から期限に近づいたサーバ証明書を検索し、サーバ証明書の識別番号を取得し、新たな失効番号として識別番号より大きな番号を失効番号として決定し失効番号蓄積手段に蓄積し、サーバ証明書情報蓄積手段を検索し、サーバ証明書の識別番号と同じかより小さな識別番号を持つサーバ証明書（以下更新対象サーバ証明書）を取り出し、更新対象サーバ証明書を持つサーバに対して新たな失効番号と同じかより大きな識別番号

を持つサーバ証明書に更新する構成としてもよい。

### 【0213】

#### 【発明の効果】

以上の説明から明らかなように、本発明に係る通信装置によれば、従来のようにサーバ証明書の有効期限が過ぎたか否かを時計を用いて判断したり、従来のようにリポジトリからサイズの大きなCRLを取得して、たくさんのリストを記憶し、このたくさんのリストの中にサーバ証明書の識別番号が載っているか否か検索したりする必要がなくなり、通信装置は、リポジトリから失効番号を1つだけ取得し、これを記憶している1つの失効番号で、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。したがって、通信装置及びリポジトリのメモリ容量などのリソースが簡単で済み、簡単なリソースでサーバ装置の正当性を示すサーバ証明書に基づいて当該サーバ装置と通信することができる。

### 【0214】

また、本発明に係る通信装置によれば、通信装置は、サーバ装置との通信と同じ手順でリポジトリ証明書を取得し、リポジトリ証明書を用いてリポジトリを認証したり、リポジトリが正当である場合に失効番号を暗号通信で取得したり、正常な失効番号だけを取得して、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。

### 【0215】

また、本発明に係る通信装置によれば、通信装置は、リポジトリが正当である場合に失効番号を暗号なしの通信で取得したり、正常な失効番号だけを取得して、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。

### 【0216】

また、本発明に係る証明書発行装置によれば、従来のようにサーバ証明書の有効期限が過ぎたか否かを時計を用いて判断させたり、従来のようにリポジトリからサイズの大きなCRLを取得させたりして、たくさんのリストを記憶させたりし、このたくさんのリストの中にサーバ証明書の識別番号が載っているか否か検

索させたりする必要がなくなり、通信装置は、リポジトリから失効番号を1つだけ取得し、これを記憶している1つの失効番号で、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。したがって、通信装置及びリポジトリのメモリ容量などのリソースが簡単で済み、簡単なリソースでサーバ装置の正当性を示すサーバ証明書に基づいて当該サーバ装置と通信することができる。

#### 【0217】

また、本発明に係る証明書発行装置によれば、有効期間が近づいたサーバ証明書を失効させることができる。

#### 【0218】

また、本発明に係る証明書発行装置によれば、サーバ装置は、新たなサーバ証明書を用いて認証を受けることができる。

#### 【0219】

よって、本発明により、極めて簡単なリソースでサーバ装置を認証することができ、インターネットが普及し、リソースが小さいネット家電装置等が登場しつつある今日における本願発明の実用的価値は極めて高い。

#### 【図面の簡単な説明】

##### 【図1】

本発明の実施の形態1に係る通信システム1の全体構成を示すブロック図である。

##### 【図2】

図1に示されるサーバ証明書75の構成例を示す図である。

##### 【図3】

図1に示される失効情報90の構成例を示す図である。

##### 【図4】

図1に示されるサーバ証明書履歴テーブル110aの構成例を示す図である。

##### 【図5】

サーバ証明書組立部107が行う証明書用シリアル設定処理の動作を示すフローチャートである。

**【図 6】**

サーバ証明書期限検索部 111 が行う証明書期限管理処理の動作を示すフローチャートである。

**【図 7】**

失効証明書検索部 113 が有効期限到来による失効証明書検索処理の動作を示すフローチャートである。

**【図 8】**

失効証明書検索部 113 が行う失効通知による失効証明書検索処理の動作を示すフローチャートである。

**【図 9】**

失効情報署名部 116 が行う失効情報組立処理の動作を示すフローチャートである。

**【図 10】**

サーバ証明書検証部 430 の各部が行う失効情報取得処理の動作を示すフローチャートである。

**【図 11】**

暗号化して通信を行う場合のシーケンス図である。

**【図 12】**

サーバ証明書検証部 430 が行うサーバ証明書 75 の検証動作を示すフローチャートである。

**【図 13】**

サーバが 4 台あったときのサーバ証明書 75 のシリアルと失効番号との関係を示す図である。

**【図 14】**

本発明の実施の形態 2 に係る通信システム 2 の全体構成を示すブロック図である。

**【図 15】**

SSL 通信時における通信システムのシステム構成を示すブロック図である。

**【図 16】**

図15に示されるサーバ証明書7000の最小限の構成例を示す図である。

【図17】

図15に示されるCRL8000の最小限の構成を示す図である。

【図18】

暗号化せずに通信を行う場合のシーケンス図である。

【図19】

暗号化して通信を行う場合のシーケンス図である。

【図20】

サーバ証明書検証部4200が行うサーバ証明書7000の検証動作を示すフローチャートである。

【符号の説明】

- 1, 2 通信システム
- 10, 11 サーバ証明書作成装置
- 20, 21 リポジトリ
- 30a～30k アプリケーションサーバ
- 40a～40n, 41a～41n 端末
- 50 インターネット50
- 60 CA証明書
- 70 CSR
- 75 サーバ証明書
- 80 失効通知
- 90 失効情報
- 90b 失効情報
- 101 鍵ペア作成部
- 102 CA証明書作成部
- 103 CA秘密鍵蓄積部
- 104 時計
- 105 シリアル蓄積部
- 106 CSR受信部

- 1 0 7 サーバ証明書組立部
- 1 0 8 署名部
- 1 0 9 サーバ証明書送信部
- 1 1 0 サーバ証明書履歴蓄積部
- 1 1 0 a サーバ証明書履歴テーブル
- 1 1 1 サーバ証明書期限検索部
- 1 1 2 サーバ証明書失効通知部
- 1 1 3 失効証明書検索部
- 1 1 4 証明書失効通知部
- 1 1 5 失効番号蓄積部
- 1 1 6 失効情報署名部
- 1 1 7 失効情報通知部
- 1 2 1 失効番号蓄積部
- 1 2 2 失効番号通知部
- 2 0 1 失効情報蓄積部
- 2 0 2 通信部
- 2 0 3 鍵ペア作成部
- 2 0 4 C S R 作成部
- 2 0 5 サーバ秘密鍵蓄積部
- 2 0 7 サーバ証明書蓄積部
- 2 0 8 失効情報蓄積部
- 2 0 9 通信部
- 3 0 1 鍵ペア作成部
- 3 0 2 C S R 作成部
- 3 0 3 サーバ秘密鍵蓄積部
- 3 0 4 サーバ証明書蓄積部
- 3 0 5 アプリサーバ部
- 3 0 6 通信部
- 4 1 0 アプリクライアント部



- 4 2 0 通信部
- 4 3 0 サーバ証明書検証部
- 4 3 1 失効情報要求部
- 4 3 2 署名検証部
- 4 3 3 C A 証明書蓄積部
- 4 3 4 署名検証部
- 4 3 5 失効番号検証部
- 4 3 6 失効番号蓄積部
- 4 3 7 証明書シリアル抽出部
- 4 3 8 失効判定部
- 4 4 0 通信部
- 4 5 0 サーバ証明書検証部
- 4 5 1 失効情報要求部
- 4 5 2 証明書シリアル抽出部
- 4 5 3 失効番号検証部



【図 2】

## サーバ証明書75

バージョン (2)	751
シリアル (0x0011)	752
署名アルゴリズム	753
発行者 (Panasign)	754
有効期間(始期/終期) (2003. 04. 01. 00. 00:…/ 2004. 05. 01. 00. 00:…)	755
名前 (針ウド映画)	756
サーバ公開鍵 (Pubk_11)	757
署名 (Sig(Seck_CA, 針ウド映画    Pubk_11))	758

【図 3】

## 失効情報 90

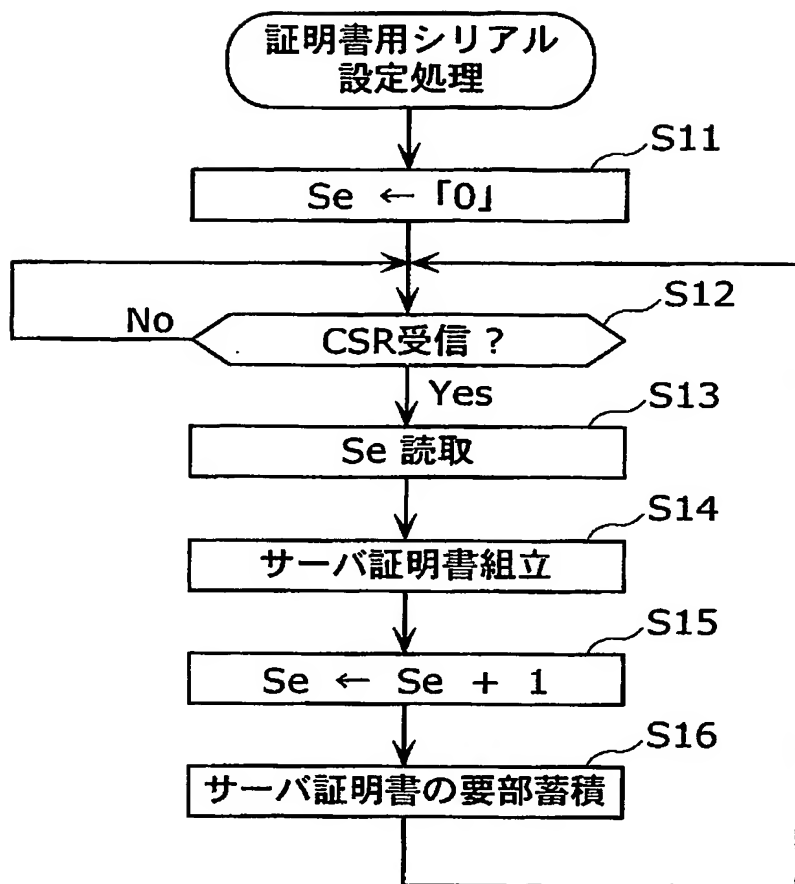
発行者 (Panasign)	91
失効番号 (0x0011)	92
署名 (Sig(Seck_CA, Panasign    0x0011))	93

【図 4】

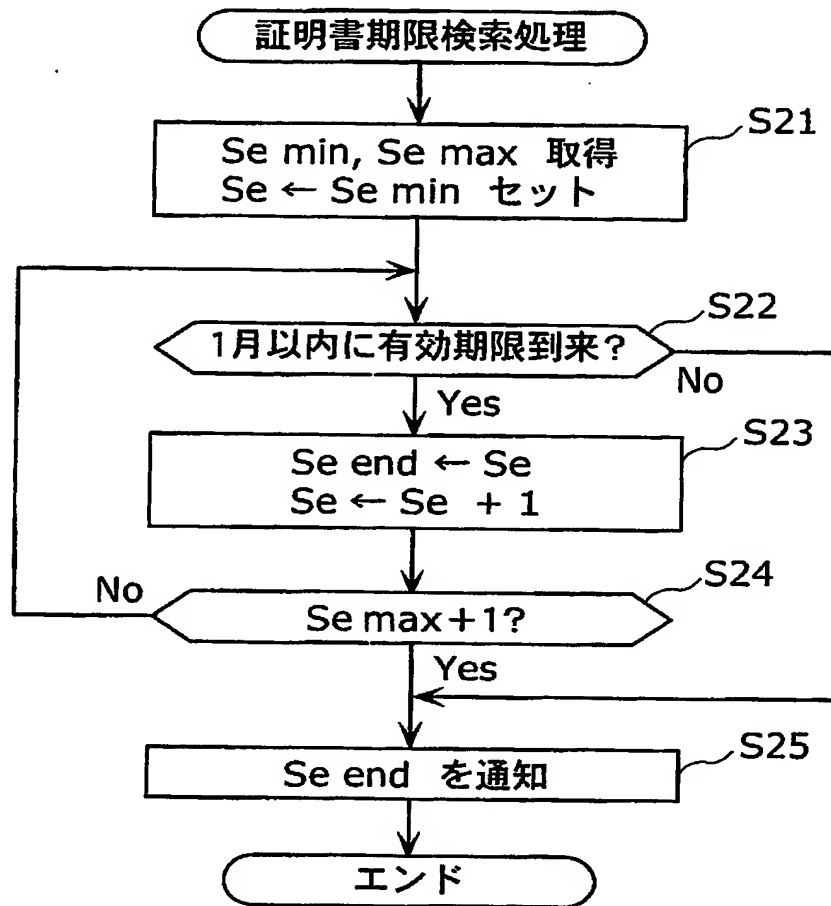
サーバ証明書履歴テーブル110a

サーバの名前	サーバ証明書のシリアル	有効期限
針ウド映画	0x0011	2003.04.11.00.00:00.00
大波ゲーム	0x0012	2003.04.11.09.23:46.00
⋮	⋮	⋮
ロボット調教師	0x0049	2003.11.03.09.23:46.00
ツツジ調理レシビ	0x0050	2003.11.11.12.51:51.18
⋮	⋮	⋮
洗濯日和	0x0110	2004.05.10.21.42:35.00

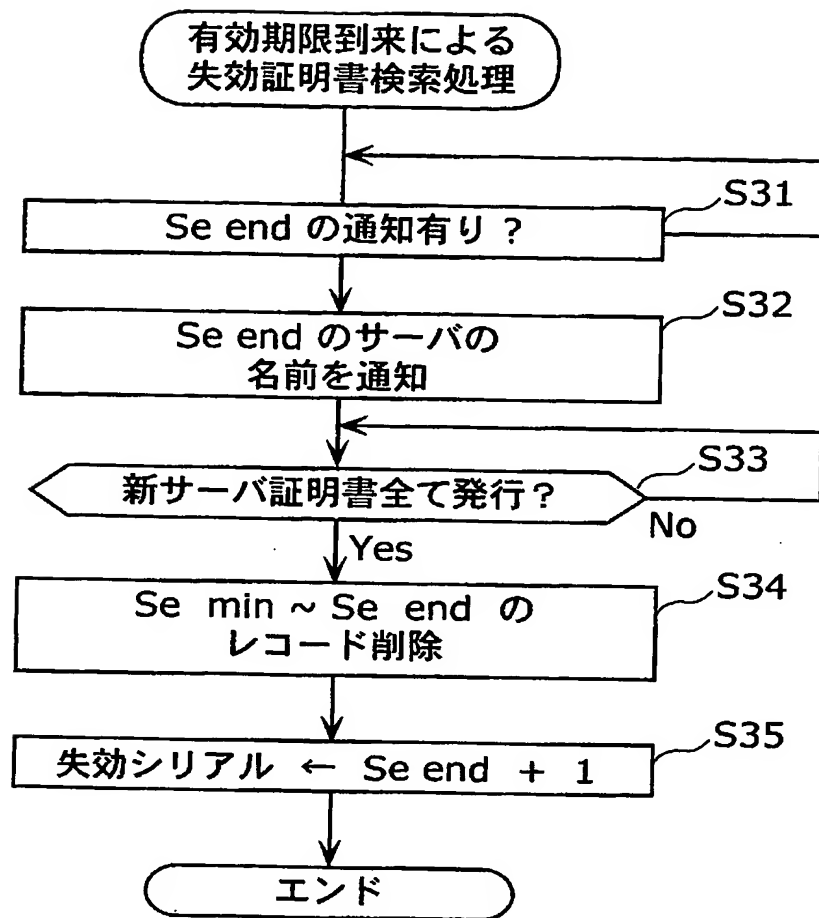
【図 5】



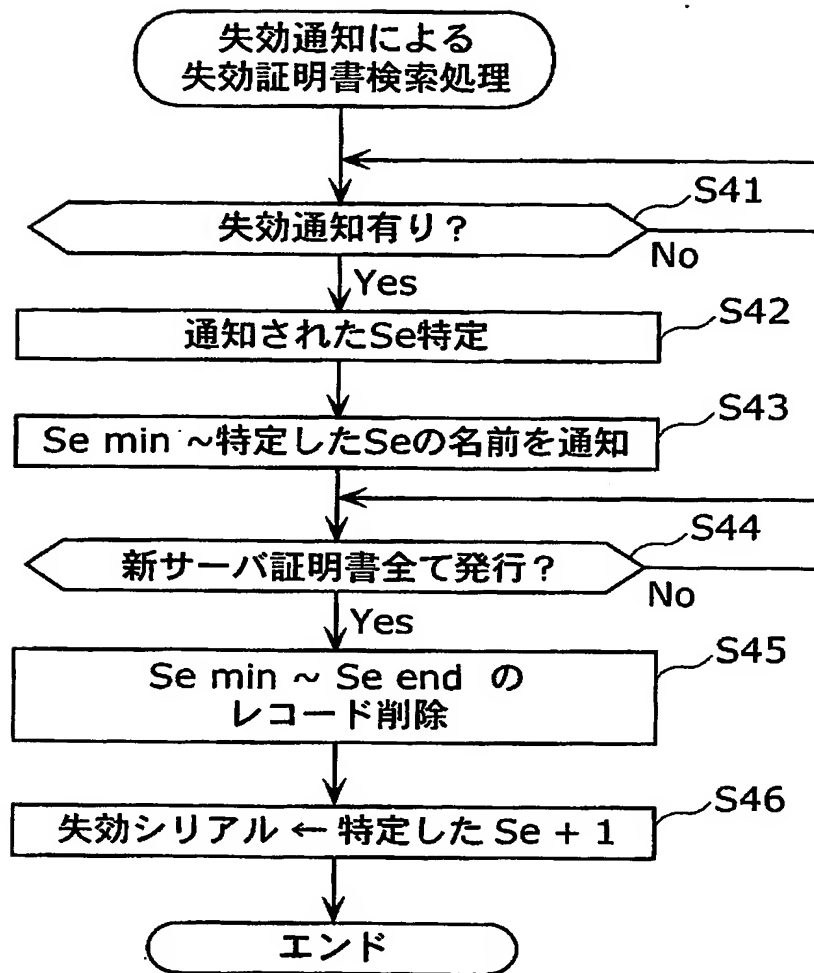
【図 6】



【図7】

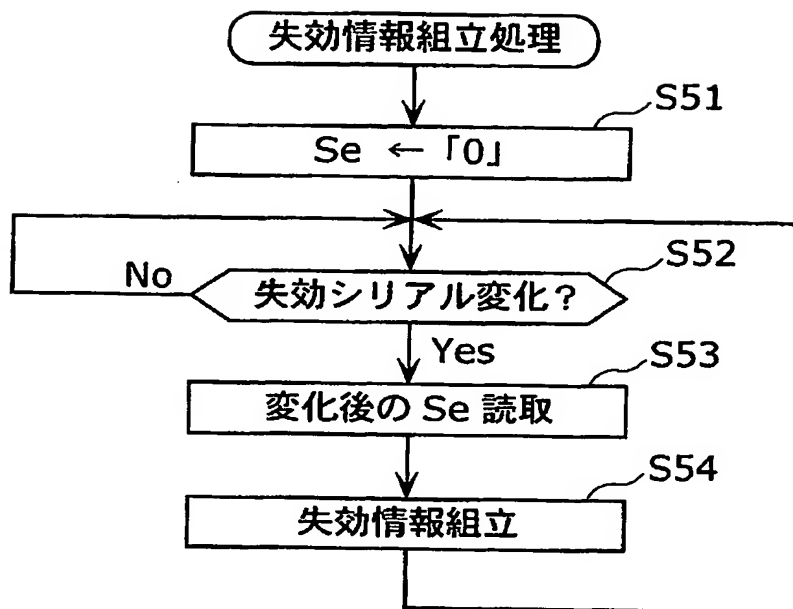


【図8】

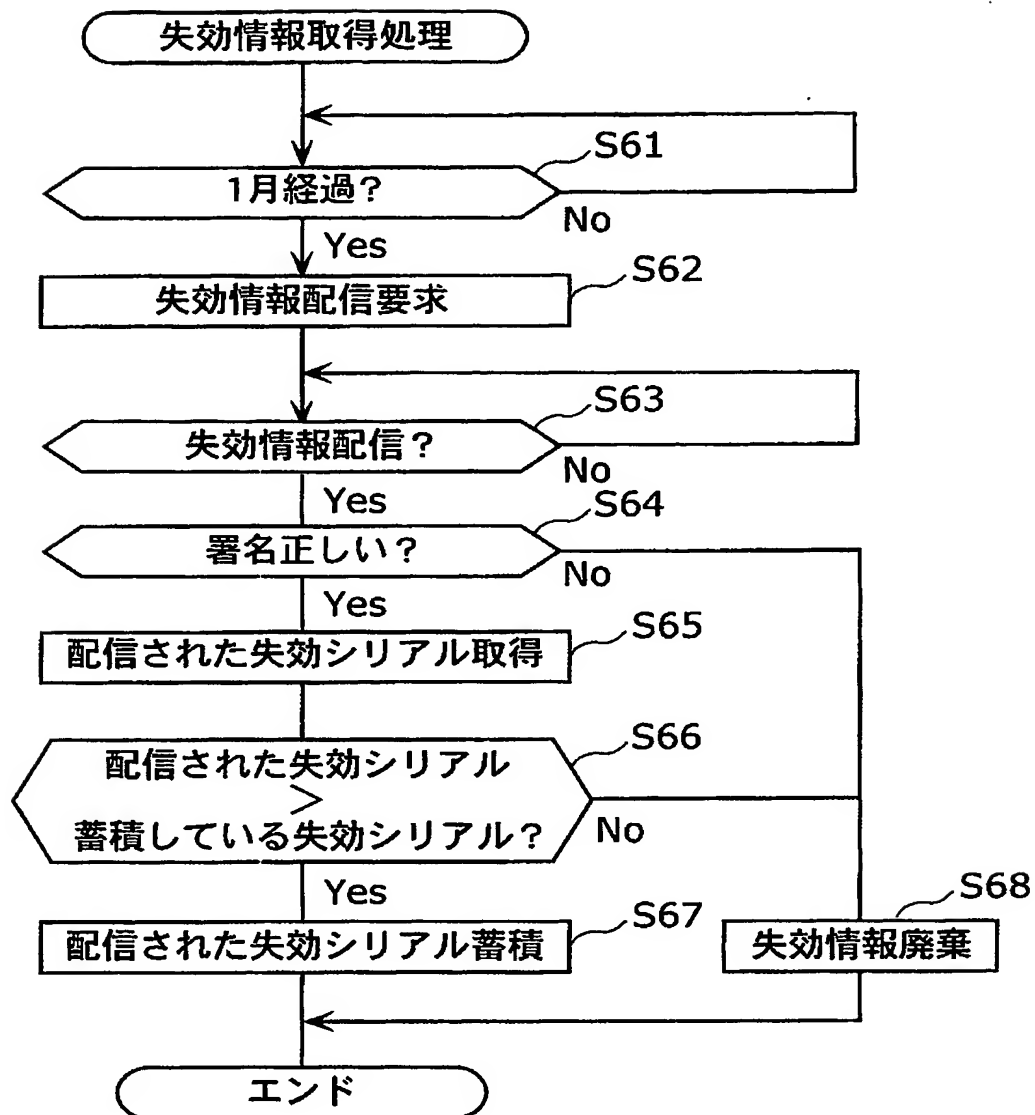




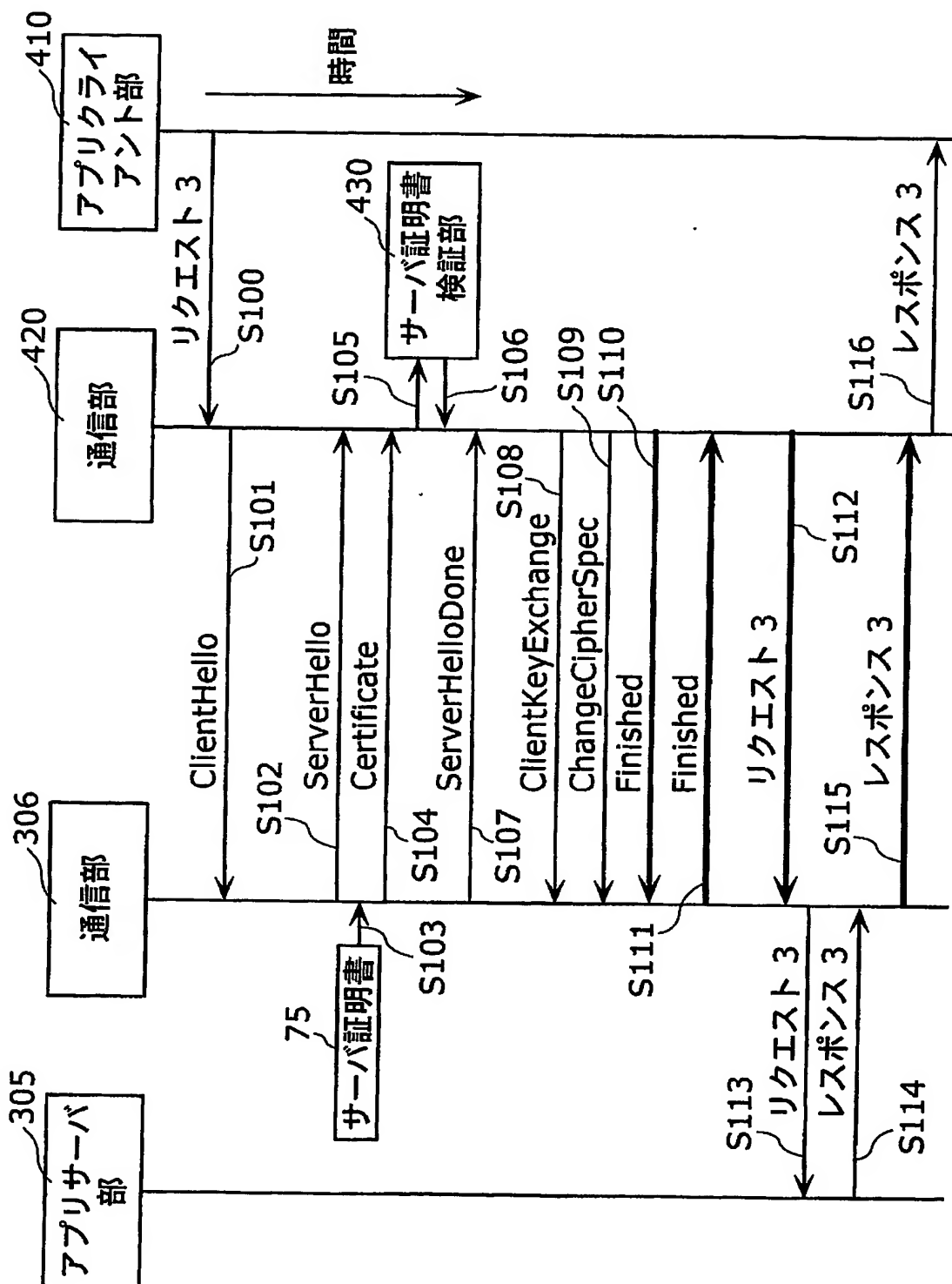
【図 9】



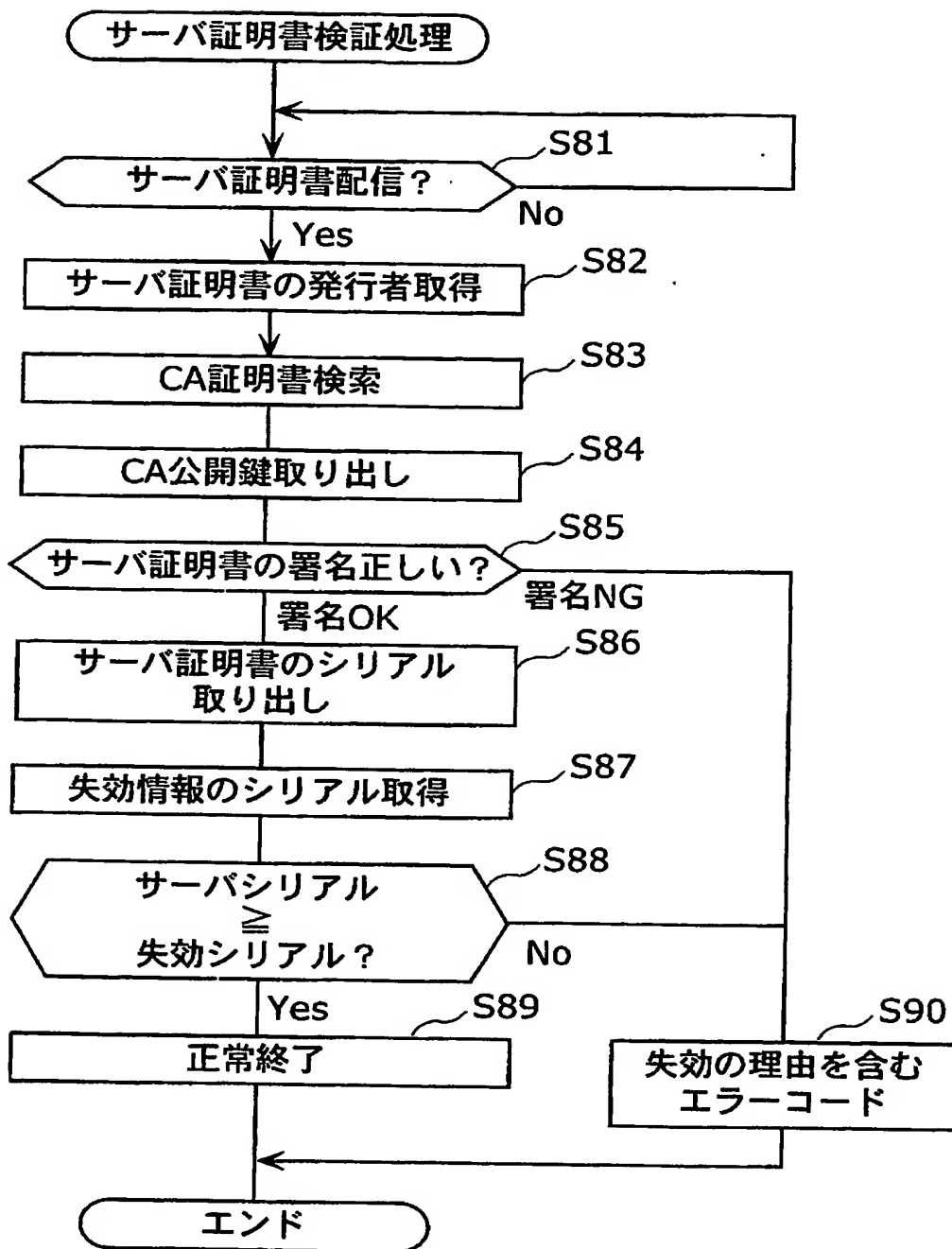
【図 10】



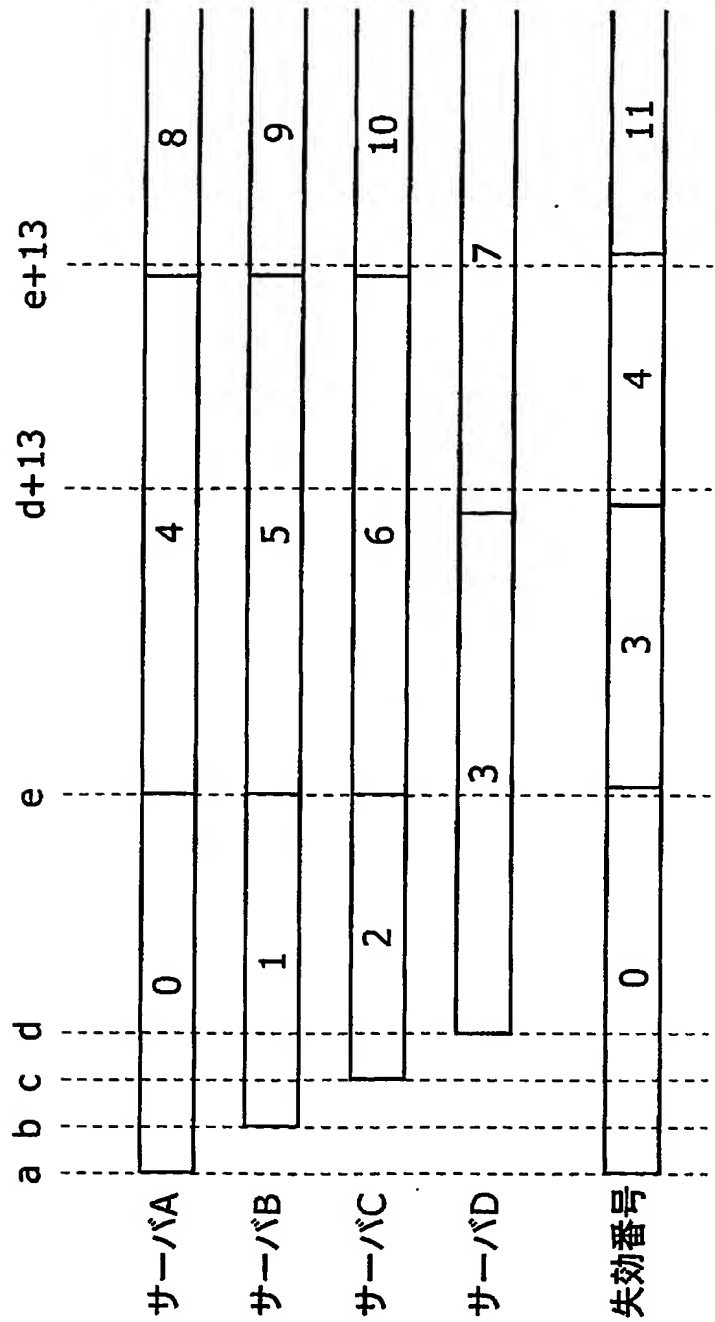
【図 11】



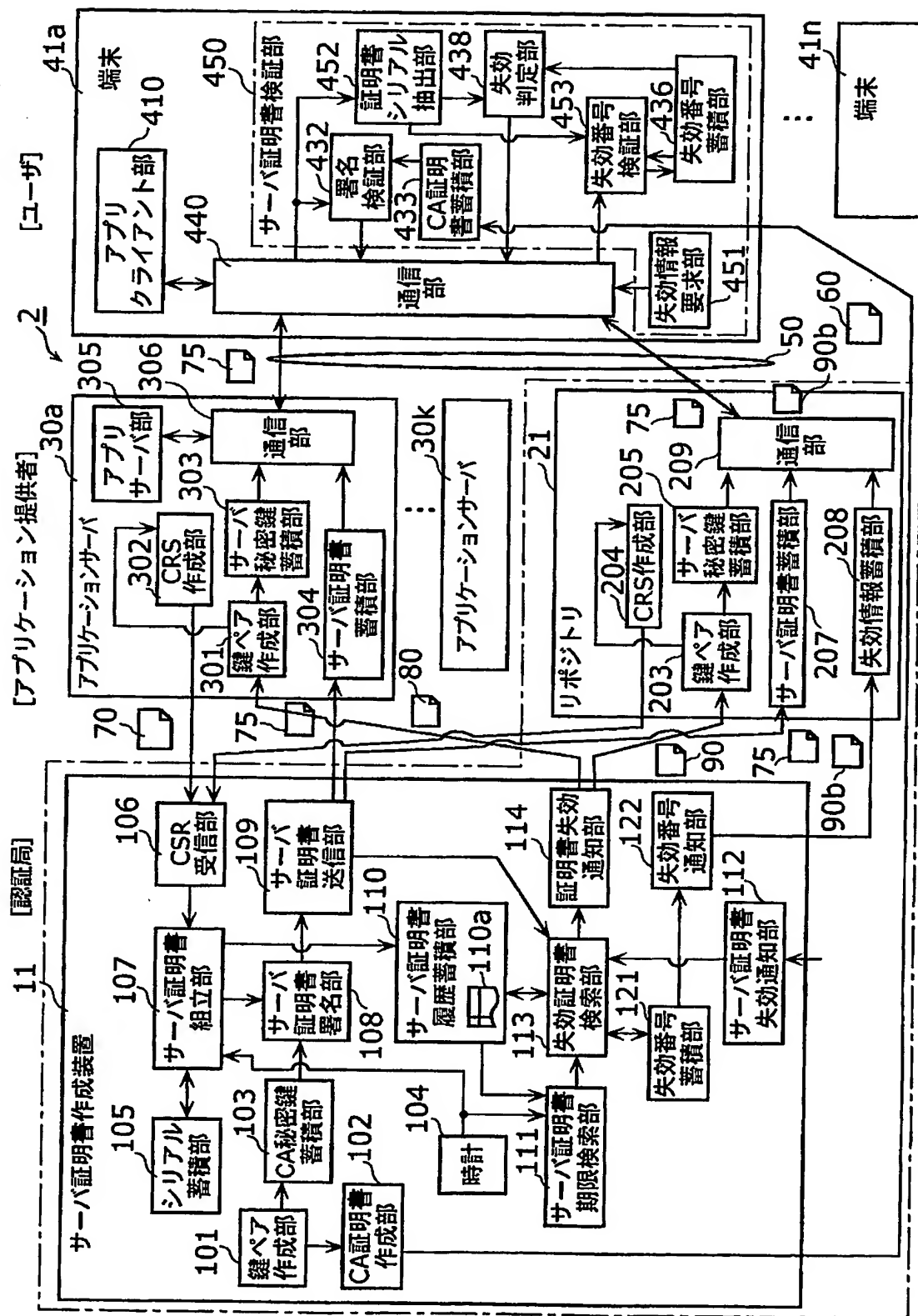
【図 12】



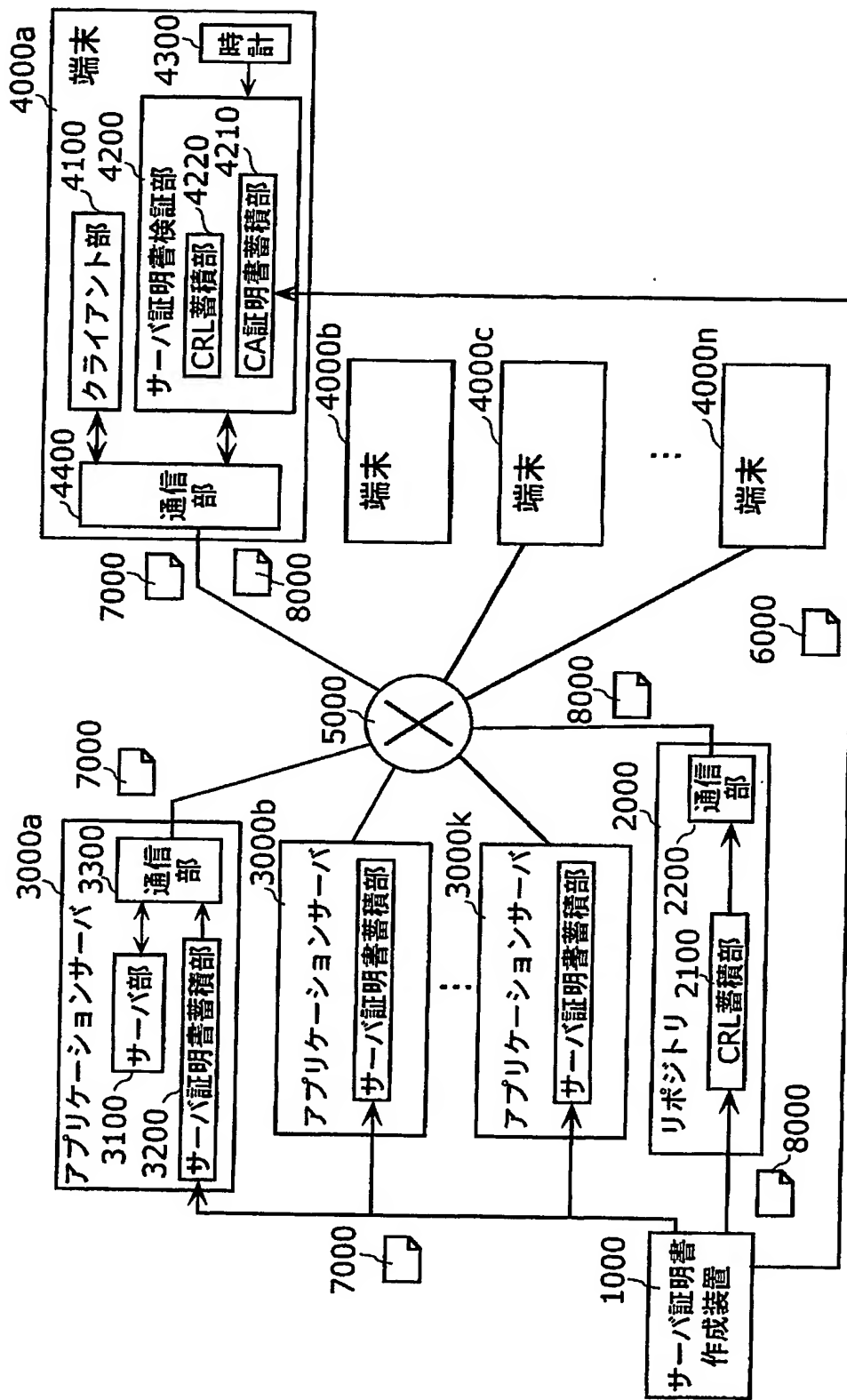
【図 13】



【図 14】



【図 15】



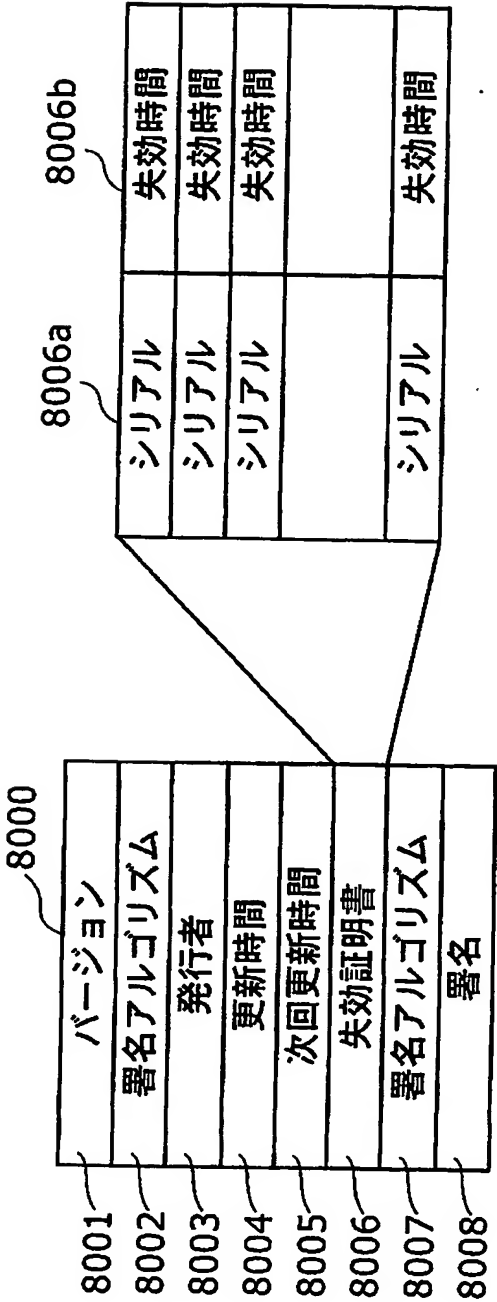
【図 16】

The diagram shows a rectangular box labeled 7000 at the top. Inside the box are eight horizontal rows, each containing a field name in Japanese. To the right of the box, there are eight pointers, each consisting of a small hook and a numerical address. The pointers are aligned with the rows of the box.

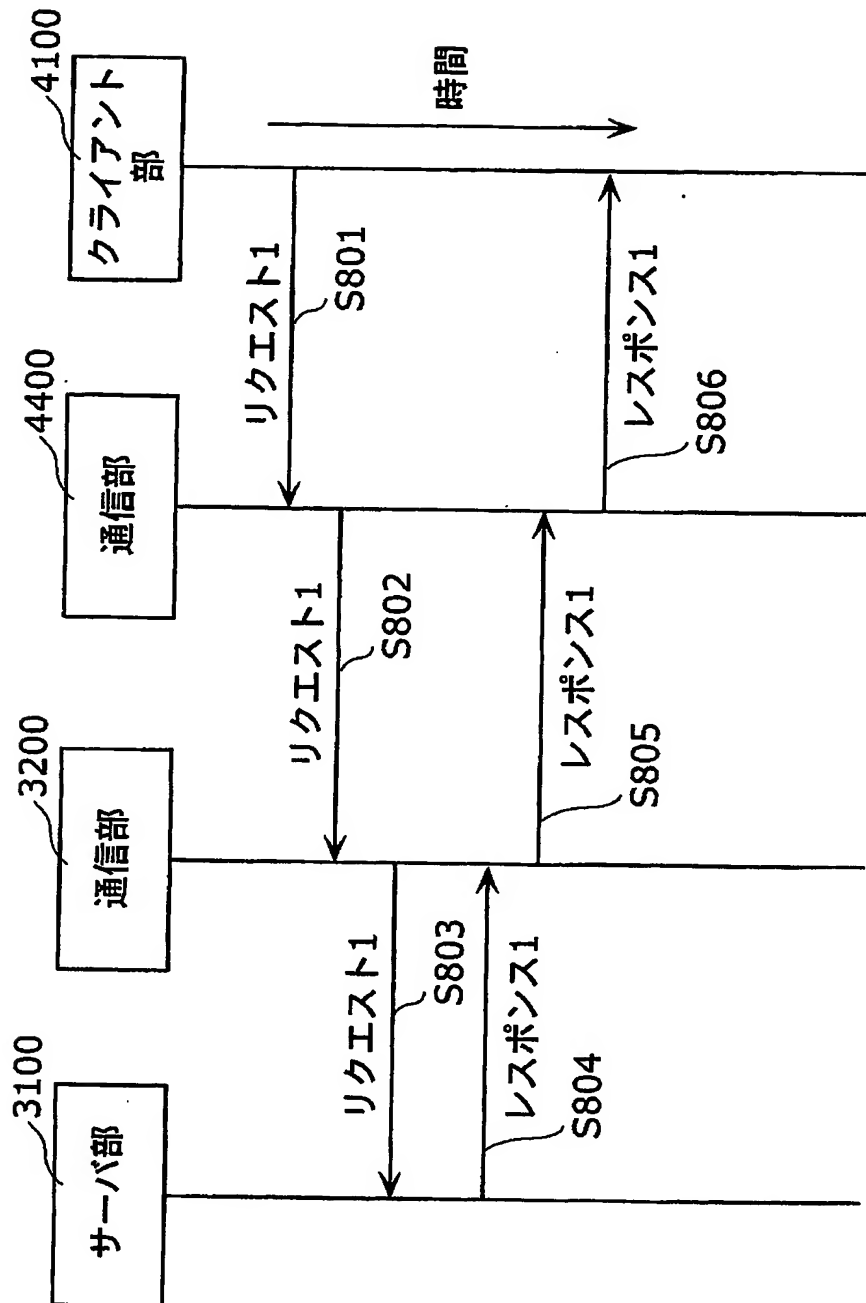
バージョン	7001
シリアル	7002
署名アルゴリズム	7003
発行者	7004
有効期間	7005
名前	7006
公開鍵	7007
署名	7008



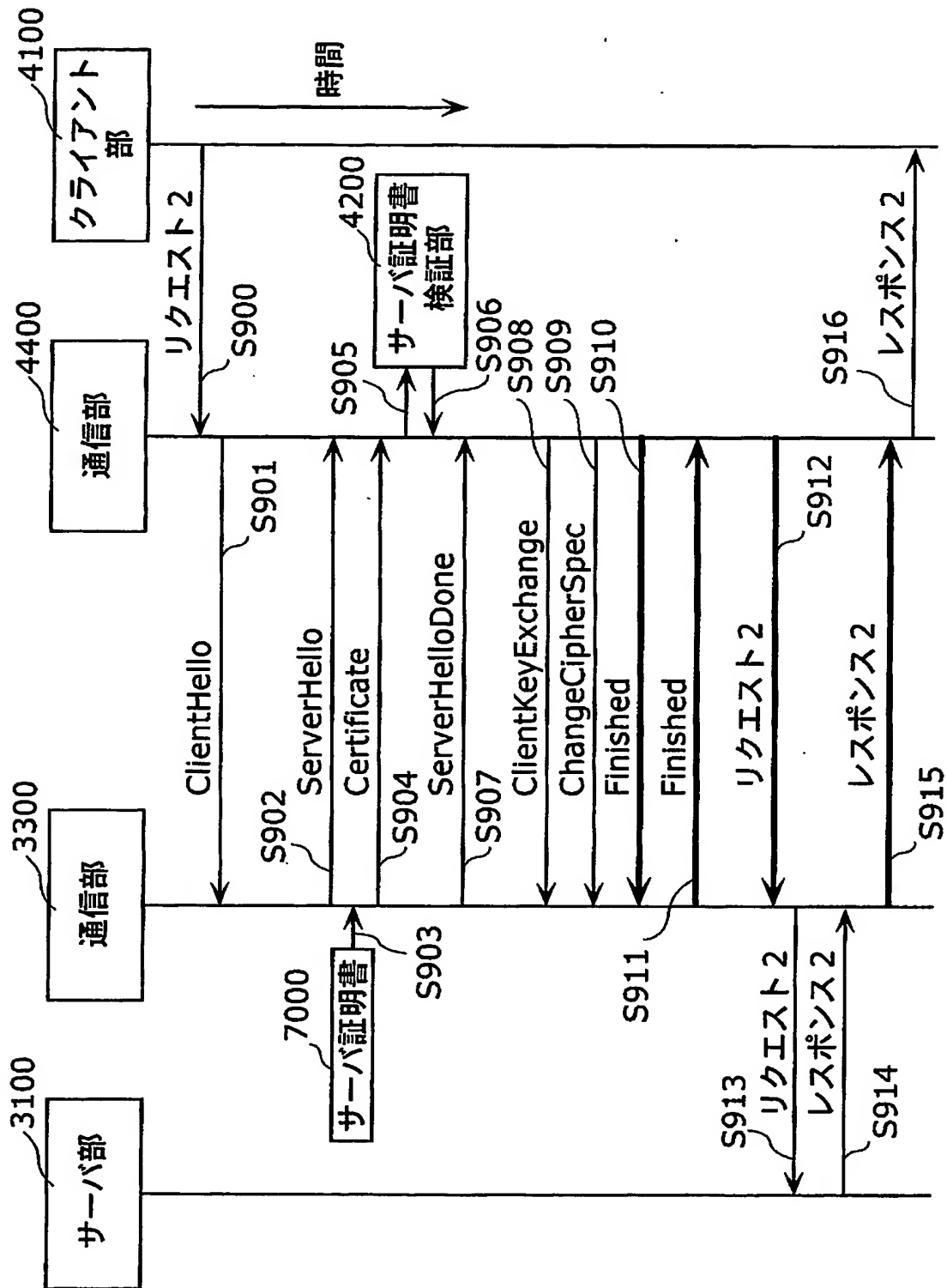
【図 17】



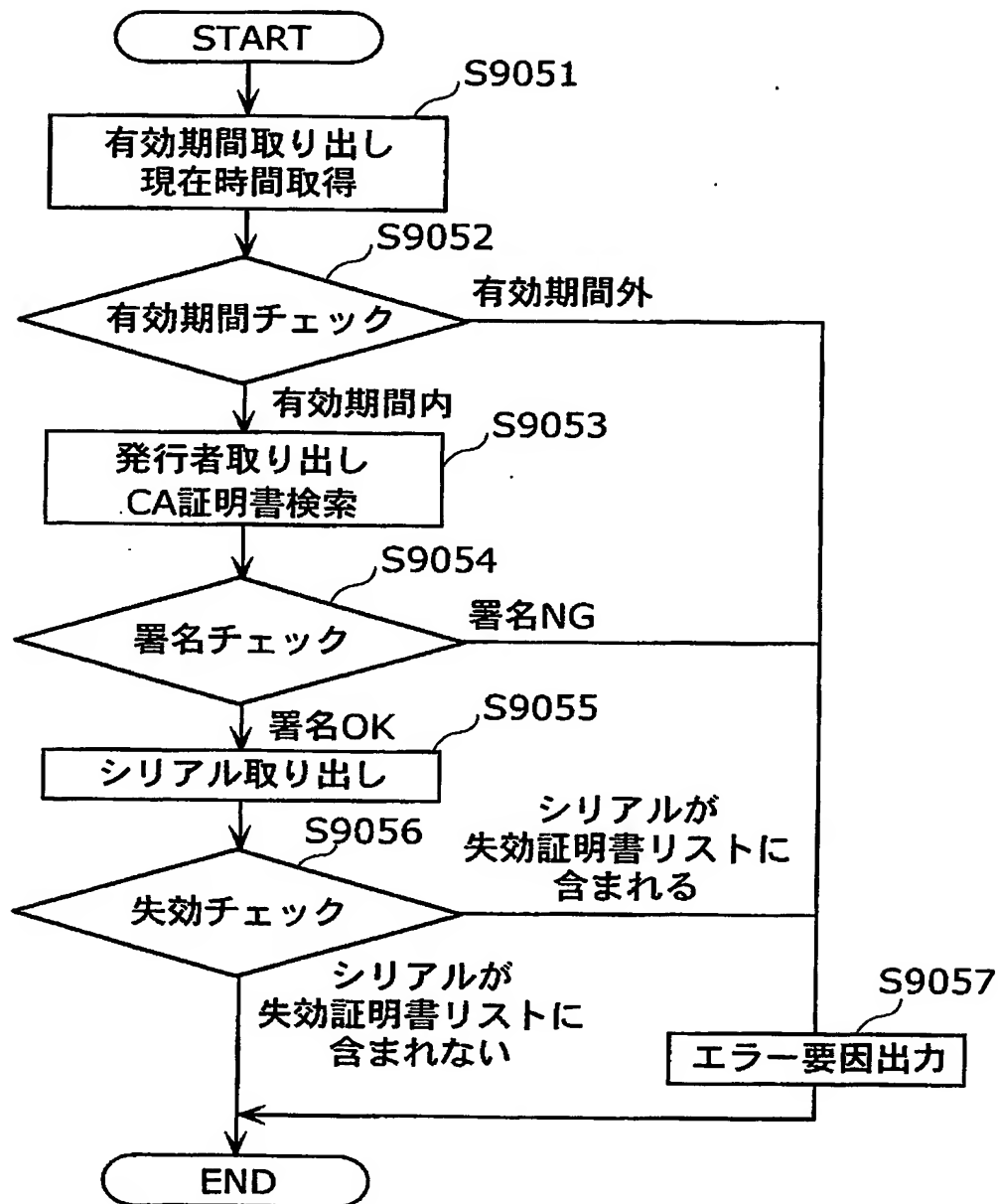
【図18】



【図 19】



【図 20】



【書類名】 要約書

【要約】

【課題】 簡単なリソースでサーバ装置の正当性を示すサーバ証明書に基づいて当該サーバ装置と通信することができる通信装置を提供する。

【解決手段】 端末 40a は、サーバ証明書 75 の有効性を判断する基準となる情報である失効番号を保持するリポジトリ 20 から、失効番号を取得する失効番号検証部 435 と、取得された失効番号を記憶する失効番号蓄積部 436 と、サーバ証明書 75 を識別する識別番号をサーバ証明書 75 から読み出す証明書シリアル抽出部 437 と、読み出された識別番号と失効番号蓄積部 436 に記憶されている失効番号とを比較することによってサーバ証明書 75 の有効性を判断する失効判定部 438 と、サーバ証明書 75 が有効であると判断された場合に、アプリケーションサーバ 30a との通信を確立し、サーバ証明書 75 が有効でないと判断された場合に、アプリケーションサーバ 30a との通信を確立しない通信部 420 とを備える。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2003-100866
受付番号	50300560470
書類名	特許願
担当官	第八担当上席 0097
作成日	平成15年 4月 4日

<認定情報・付加情報>

【提出日】	平成15年 4月 3日
-------	-------------

次頁無

特願 2 0 0 3 - 1 0 0 8 6 6

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 8 2 1 ]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社